TRUSTED
COMPUTER SOLUTIONS

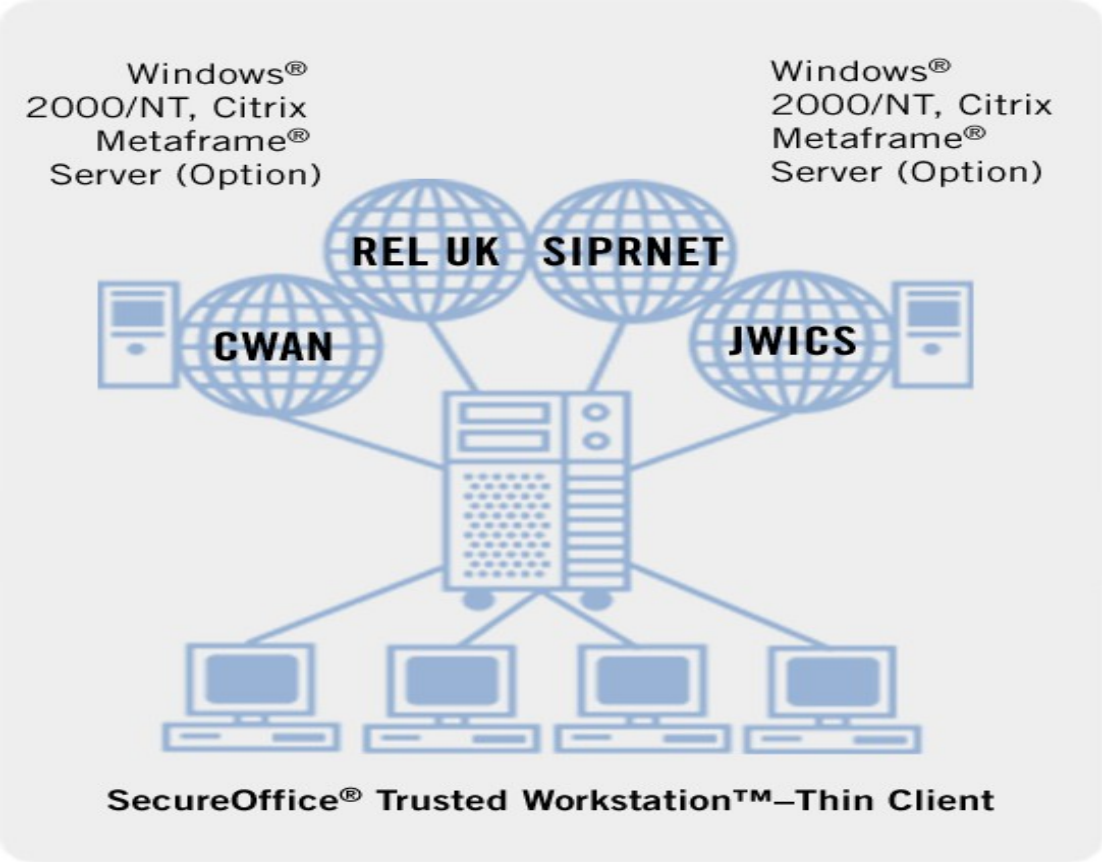
SecureOffice® Trusted Workstation™
User Training

Trusted Computer Solutions, Inc.
2350 Corporate Park Drive Suite 500
Herndon, VA 20171 USA
+1.703.318.7134 (Phone)
+1.703.318.5041 (Fax)
www.TrustedCS.com

SecureOffice® Trusted Workstation™ (TWS) User

- Trusted Operating System Overview
- Desktop Features and Conventions
- File Movement
- Integrated Applications
- Integrated Hardware

TWS Architecture



- Trusted Operating System Overview
  - TWS runs on Trusted Solaris
    - The operating system is based on UNIX
    - Supports traditional UNIX features like Discretionary Access Control (DAC)
    - Includes additional evaluated security features that allow the system to connect to multiple networks at different classification levels.
      - Mandatory Access Controls (MAC)

- Discretionary Access Controls (DAC)
  - Discretionary Access controls from standard UNIX.
  - Permissions for the Owner, Group and World (other) of a file
  - Read, Write, Execute permissions on a file (rwx)
    - File permissions example: -rw-r-----
      - » Bit 1 '-' (File Type: '-' represents normal file)
      - » Bit 2-4 'rw-' (Owner: Read, Write, No Execute)
      - » Bit 5-7 'r--' (Group: Read, No Write, No Execute)
      - » Bit 8-10 '---' (Others: No Read, No Write, No Execute)
  - Read, Write, Search permissions on a directory (rwx)
    - Directory permissions example: drwxr-x---
      - » Bit 1 'd' (File Type: 'd' represents directory)
      - » Bit 2-4 'rwx' (Owner: Read, Write, Search)
      - » Bit 5-7 'r-x' (Group: Read, No Write, Search)
      - » Bit 8-10 '---' (Others: No Read, No Write, No Search)

Discretionary Access Controls (DAC)
Setting DAC Permissions

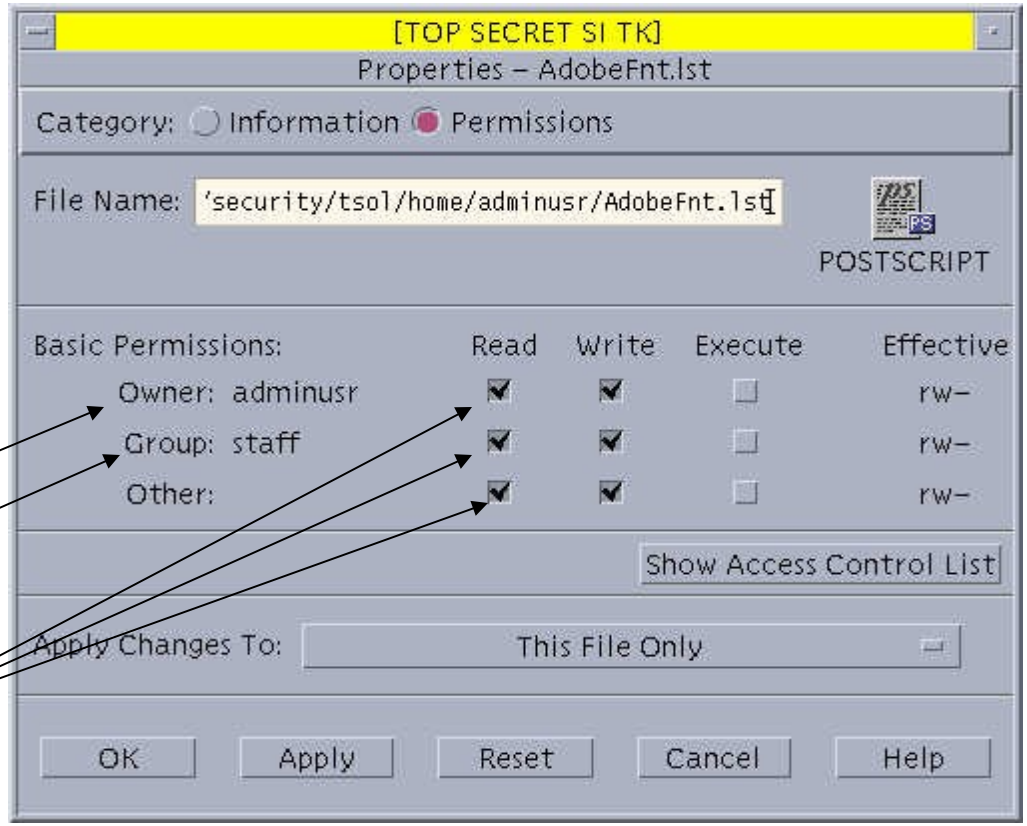
Access this file/directory properties window from file manager:

Right Click on file/directory icon, select **Properties** from the pop-up menu.

File Owner

File Group

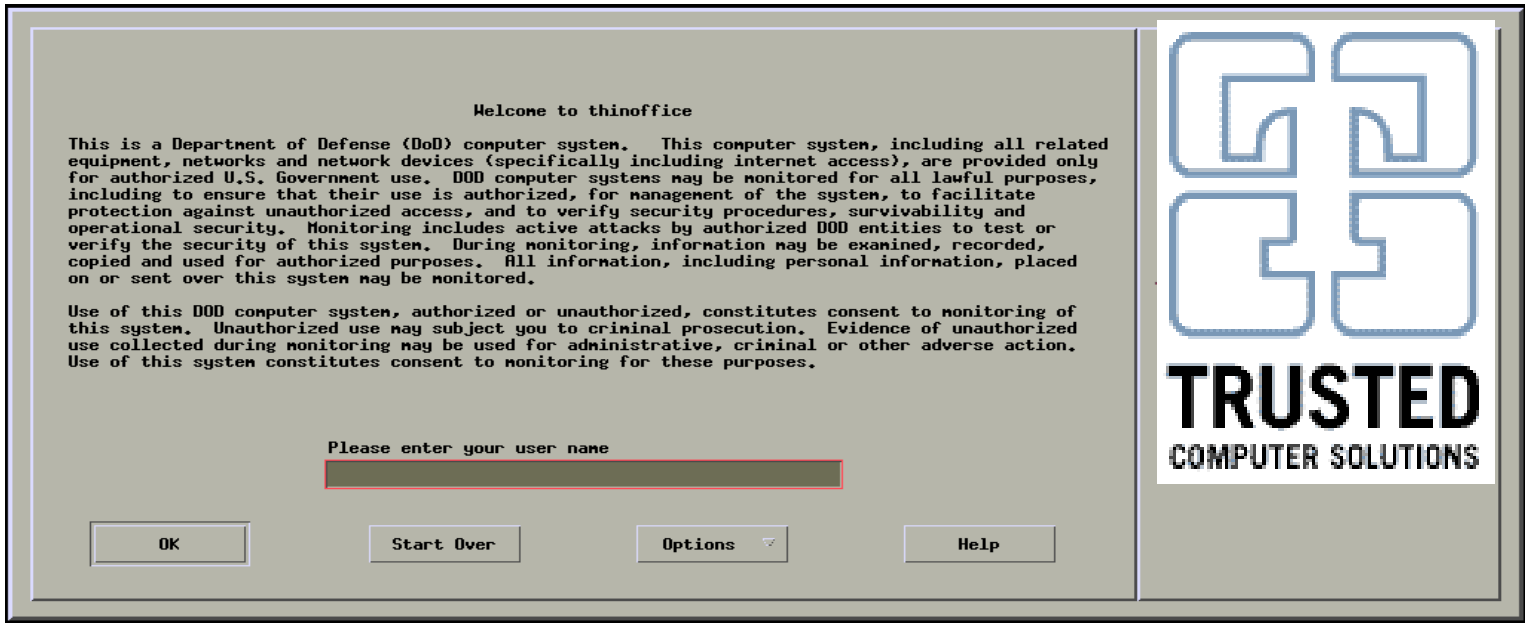
File Permissions



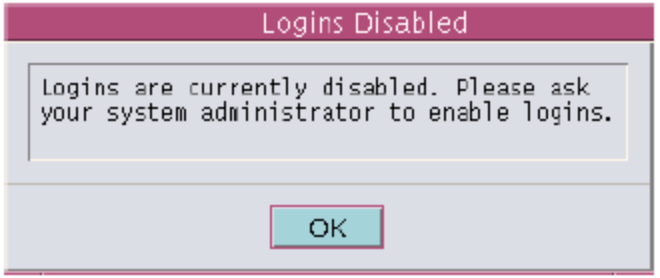
- Mandatory Access Controls (MAC)
  - Provide the “levels” in Multi-level operating systems.
    - Subjects – Typically processes or applications running on behalf of the user
    - Objects – Typically files
  - A Subjects “level” must dominate or equal the Objects “level”
  - You can read down; read up requires a privilege
  - You can write equal; write down requires a privilege.
  - DAC and MAC access control polices are complimentary.
    - A subject that dominates an object can read down without privilege assuming that it has DAC read permissions on the object.

- Auditing
  - Trusted Solaris provides very fine grain auditing capabilities
  - All users are subject to audit record collection for later analysis
  - Vast majority of actions on workstation are audited for accountability.

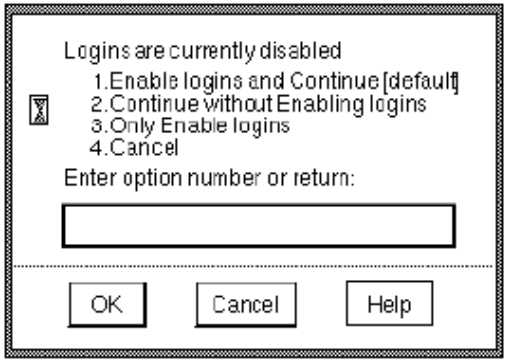
- Desktop Features and Conventions
  - System Login Process
    - Login to system with username and then enter your password when prompted at the next screen



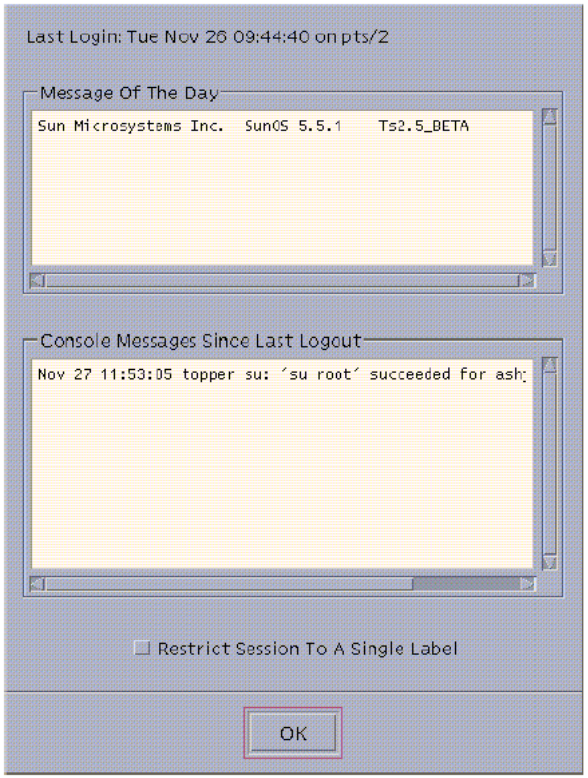
- System Login Process (con't)
  - If first to log in after reboot, logins have to be enabled.
    - If not authorized to enable logins you will see the following screen. Contact your System Administrator to have logins enabled.



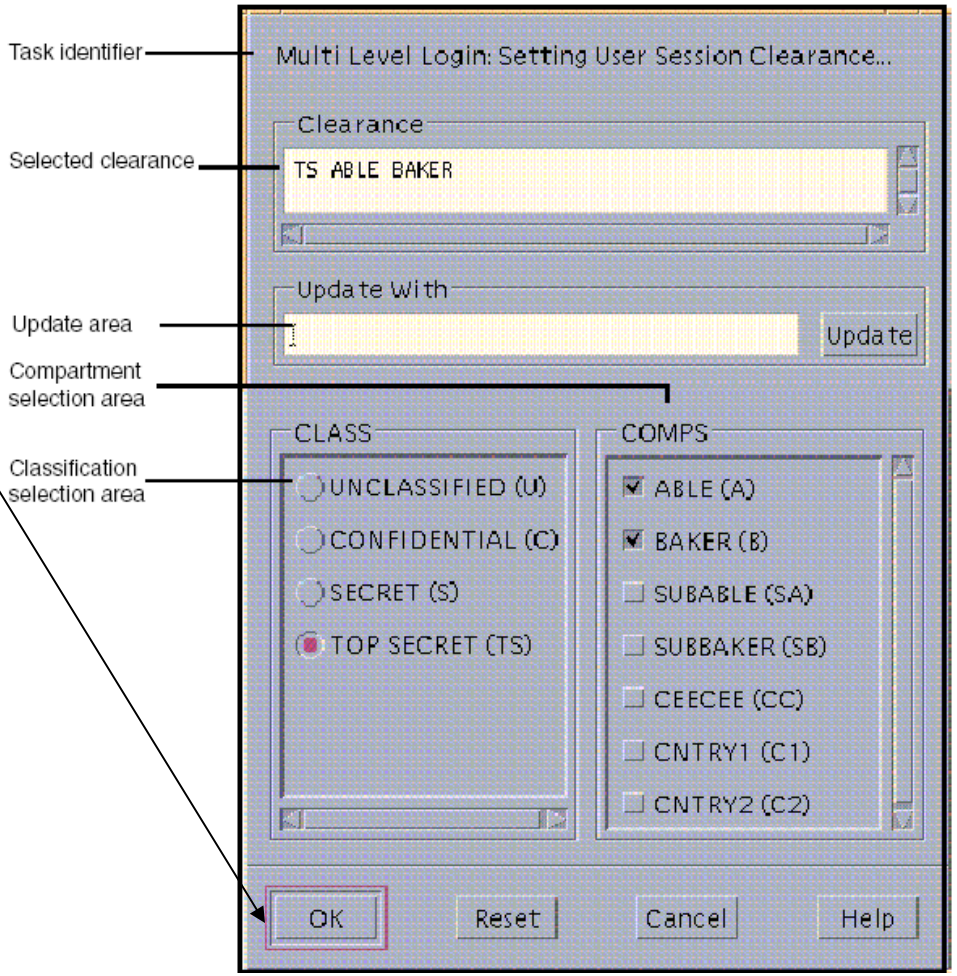
- If authorized to enable logins you will see the following screen.
  - Type option "**1**" to enable logins and press **Enter** key to continue.



- System Login Process (con't)
  - Message of the day and any console messages since the last login. Click **OK**.



- System Login Process (con't)
  - Press **OK** to accept the default settings.
  - This will allow you to access data and networks at all levels that you are authorized access to.



Common Desktop Environment (CDE)

Front Panel

Share Folder

Citrix

Application Manager

Home Folder

Screen Lock

Virtual Workspace Buttons

Relabeler

Answerbook Documentation

Relabeler Folder

Trusted Stripe

Trusted Path (Blank spaces on middle panel section)

Exit button (Logout)

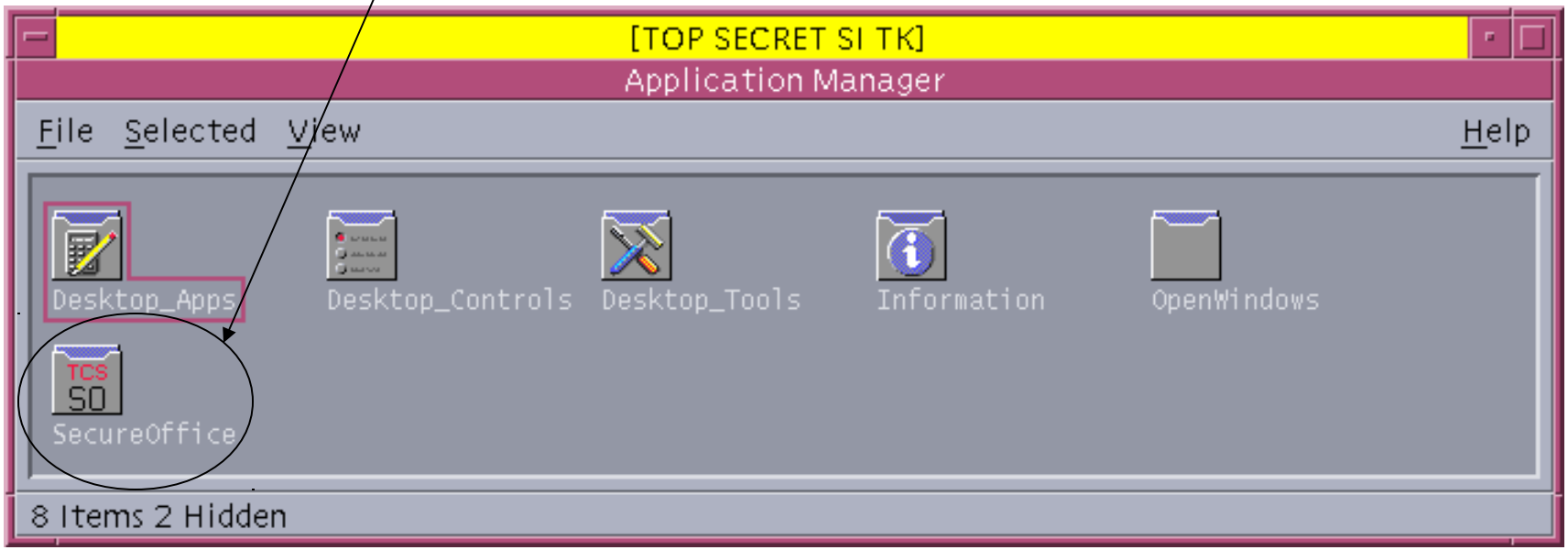
Trash

- Trusted Path
  - Direct link to system Trusted Computer Base
  - Start by right clicking in area between virtual workspaces on CDE front panel
  - Add Workspace
  - Assuming Roles (if user is authorized)
  - Change Password
  - Allocate Devices
  - Shutdown (if user authorized)
- Trusted Stripe
  - Stripe running along bottom of screen
  - Always visible
  - Indicates “Window SL” of mouse pointer
  - “Trusted Path” indicator

- The Desktop
  - Starting the Desktop
    - Left mouse click on the Application Manager icon on the CDE Front Panel

Single Click Application Manager Icon

- Starting the Desktop (con't)
  - Left mouse double-click on the SecureOffice Icon in the Application Manager



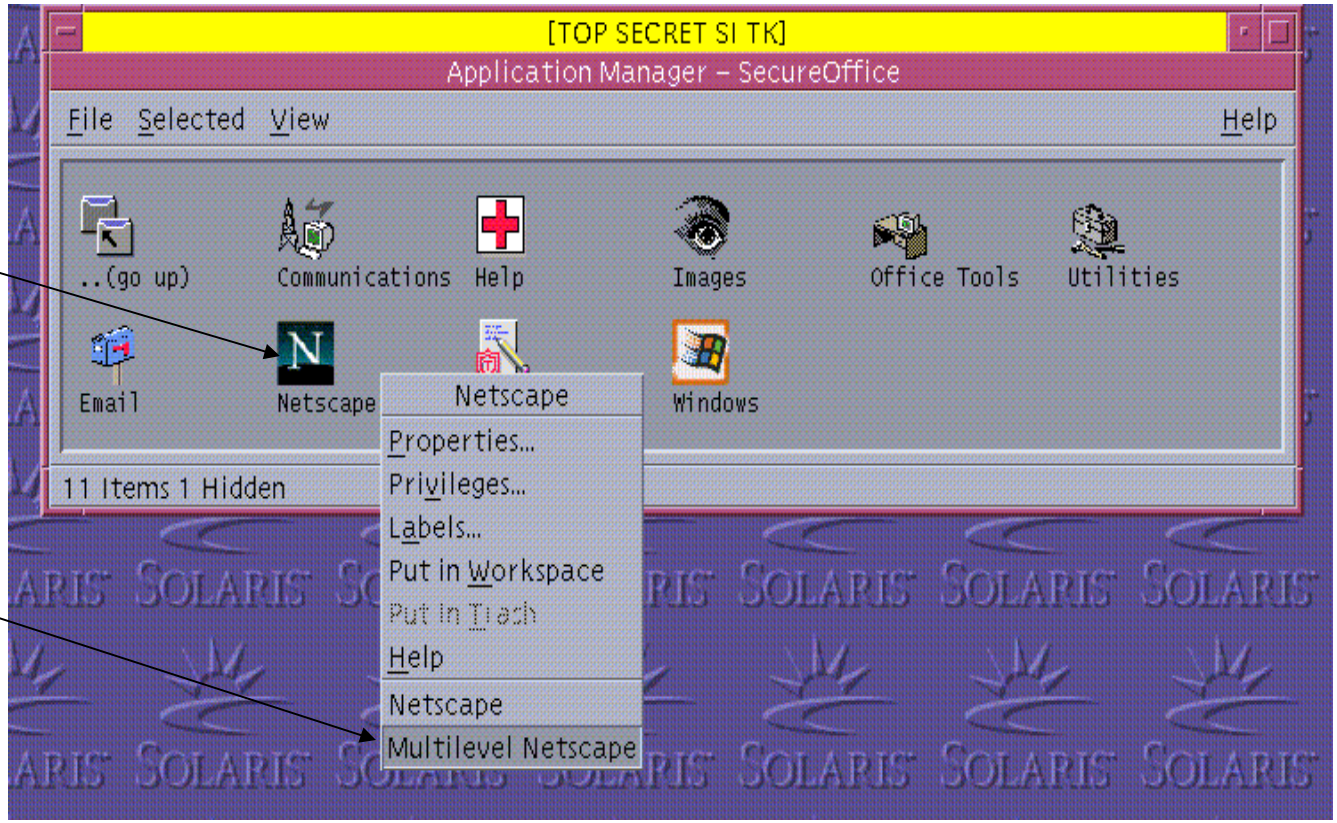
The Main Application Desktop

- Netscape Communicator
- Adobe Acrobat Reader
- ImageMagick
- Windows - Citrix Client
- Sun StarOffice
- rdesktop - optional
- MATE - NITF viewer
- XFTP
- X3270
- Sun SunForum
- INSO QuickView+
- Trusted File Relabeler

Launching Applications

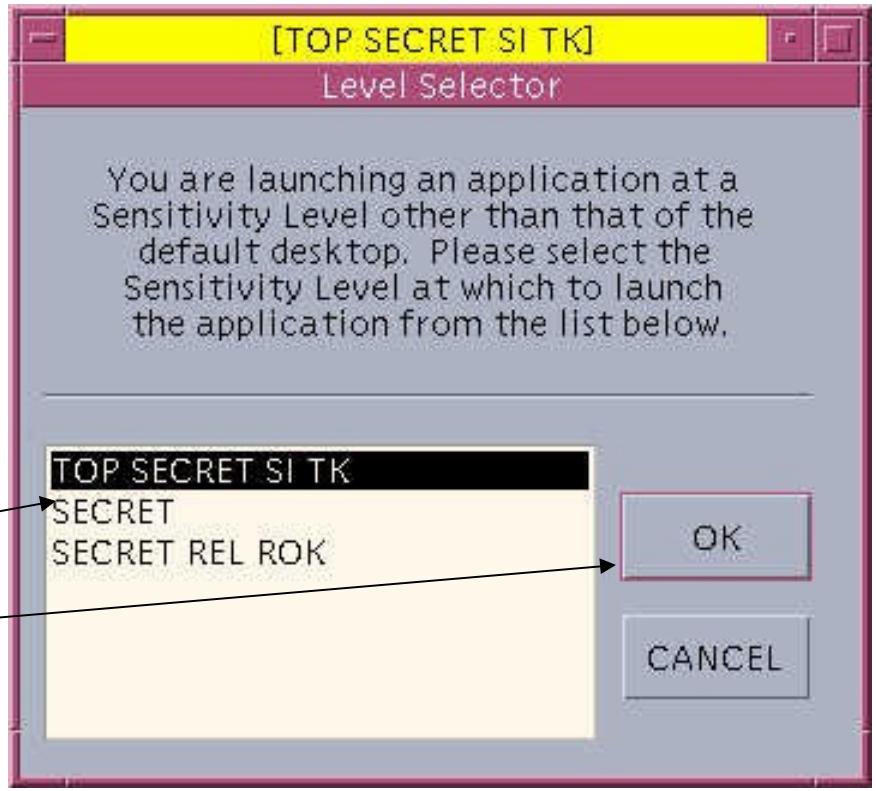
Applies to all desktop applications

- Netscape @ TS SI TK, left double-click **Netscape** icon
- Netscape @ different SL, right single-click **Netscape** icon. Select **Multilevel Netscape**



Launching Applications

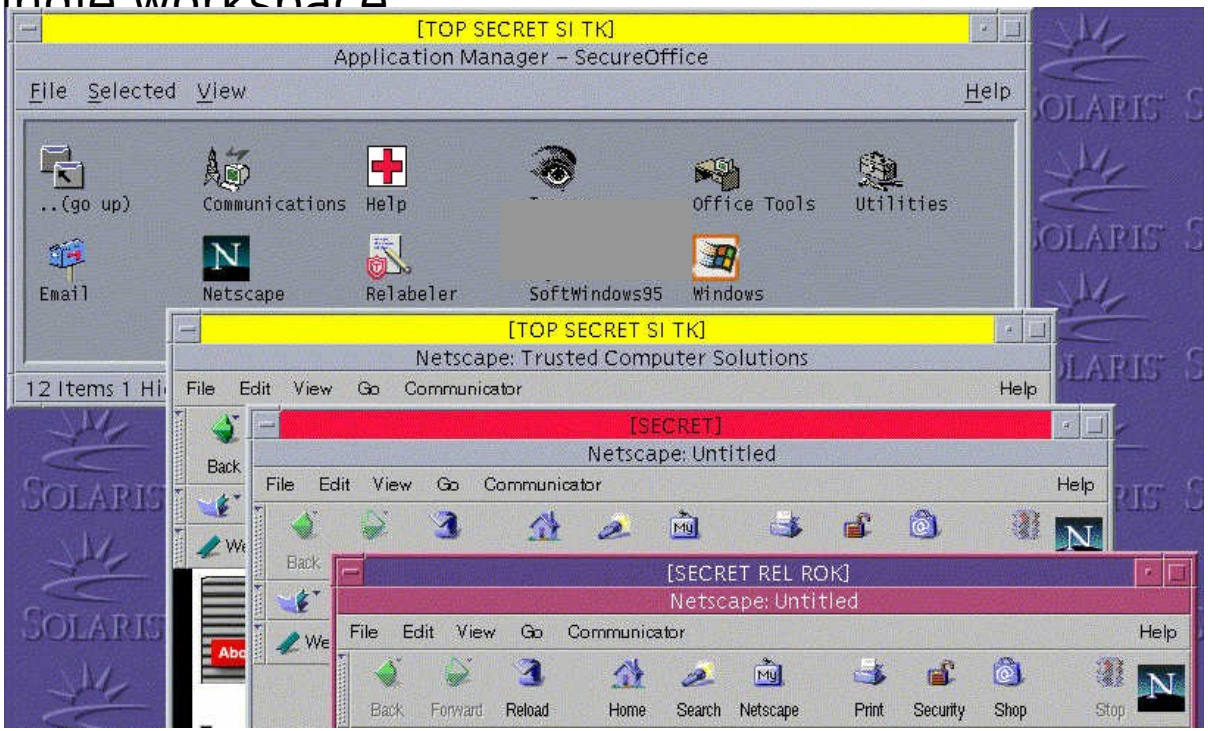
Level Selector



- Select appropriate SL from Level Selector
- Press **OK** button.
- Application will be run at specified level

Multiple Multi-Level Windows

SecureOffice can support multiple windows or applications at multiple levels simultaneously in a single workspace



- The Desktop (con't)
  - File Management
    - Concept
      - » User files can be stored at any level in the site accreditation range
      - » SECRET applications will save files as SECRET level files
      - » TOP SECRET applications will save files as TOP SECRET files
    - Common directories used for storing files
      - » Multi-Level "Home" Directory
      - » Multi-Level "Share" Directory
    - Viewing Directories at different Sensitivity Levels

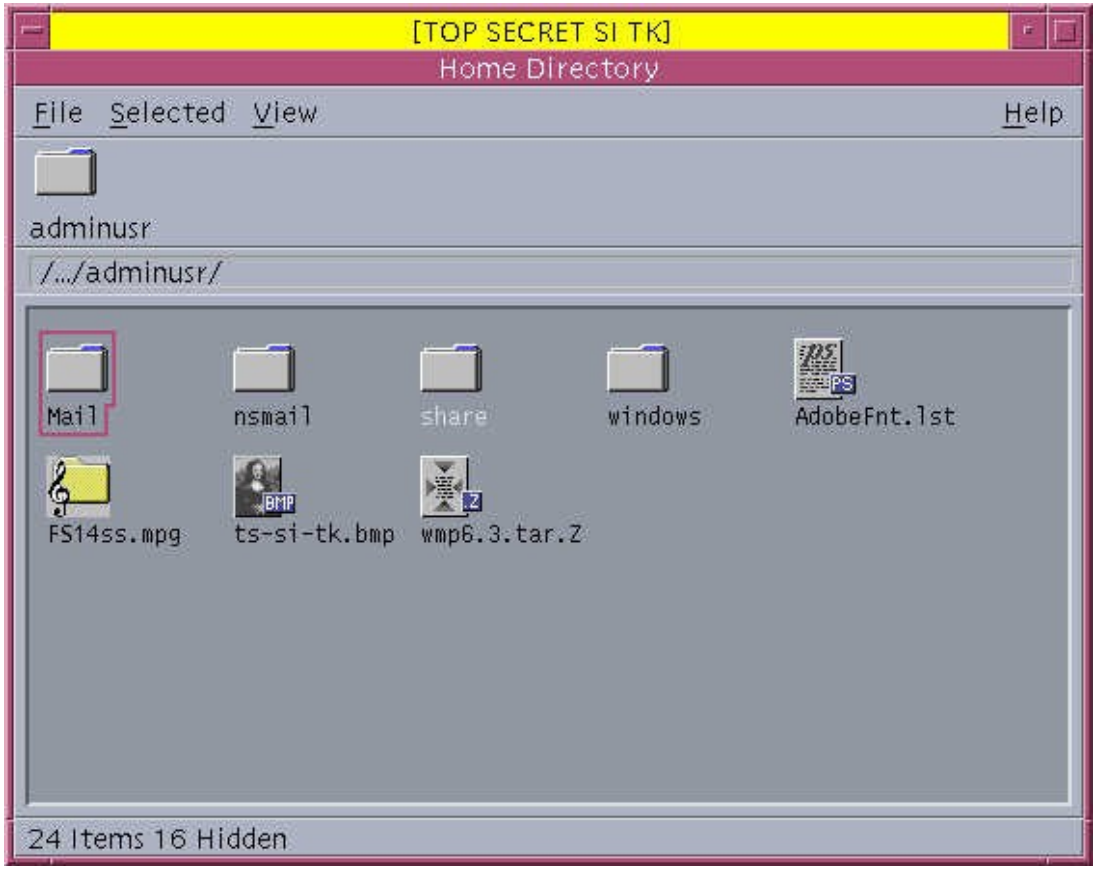
Launching a File Manager for your Home directory at the desktop workspace SL

Left single-click here to launch Home directory file manager at current workspace SL

Launching a File Manager for your Home directory at a specified Sensitivity Level

1. Click here to get the pop up menu

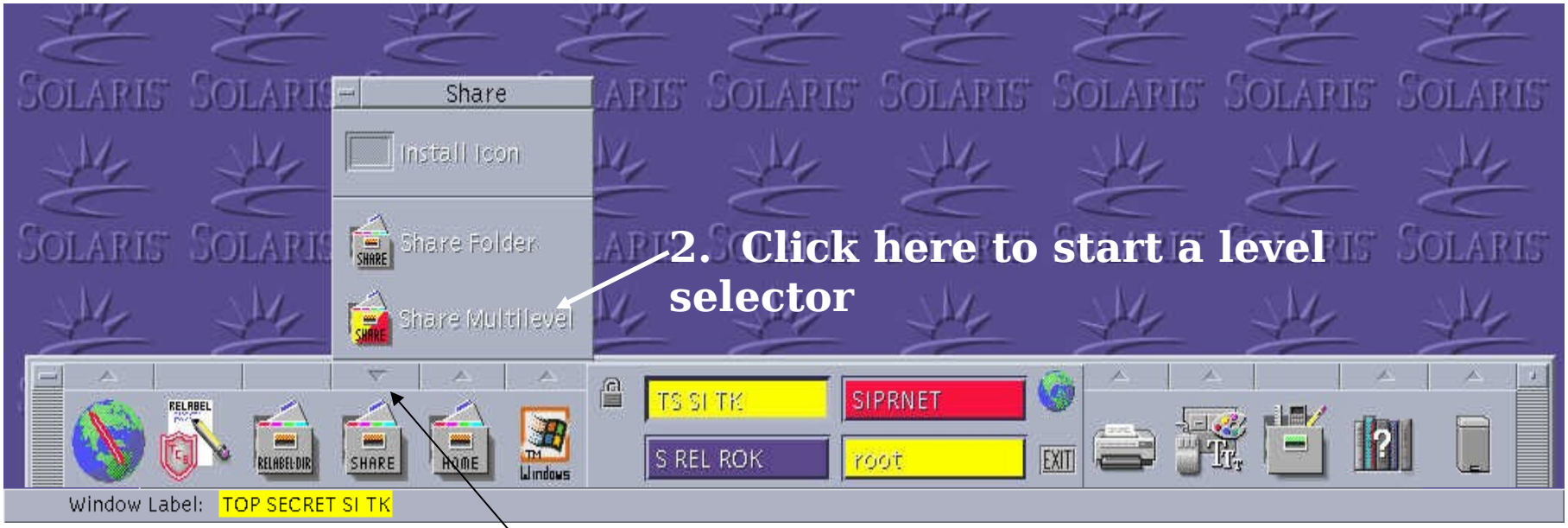
TS SI TK Home Directory File Manager



Launching a File Manager for your Share directory at the desktop workspace SL

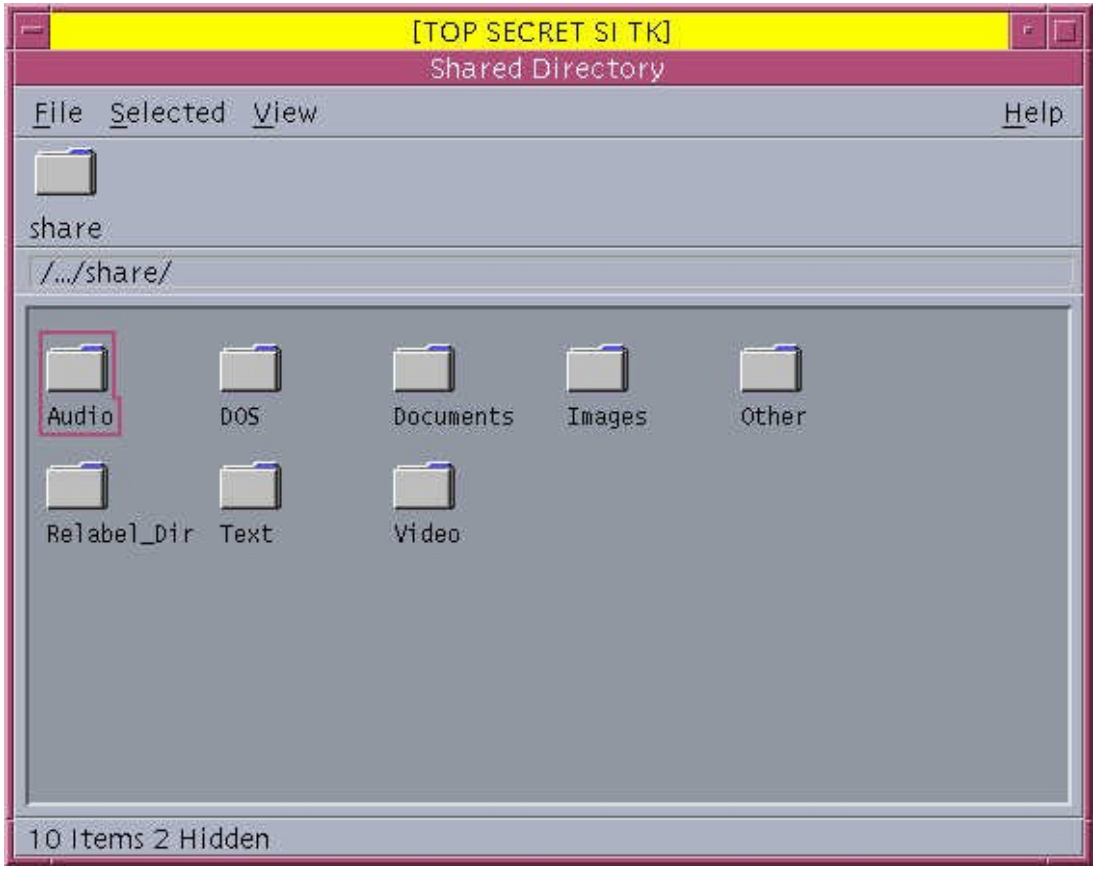
Left single-click here to launch Share directory file manager at current workspace SL

Launching a File Manager for your Share directory at a specified Sensitivity Level

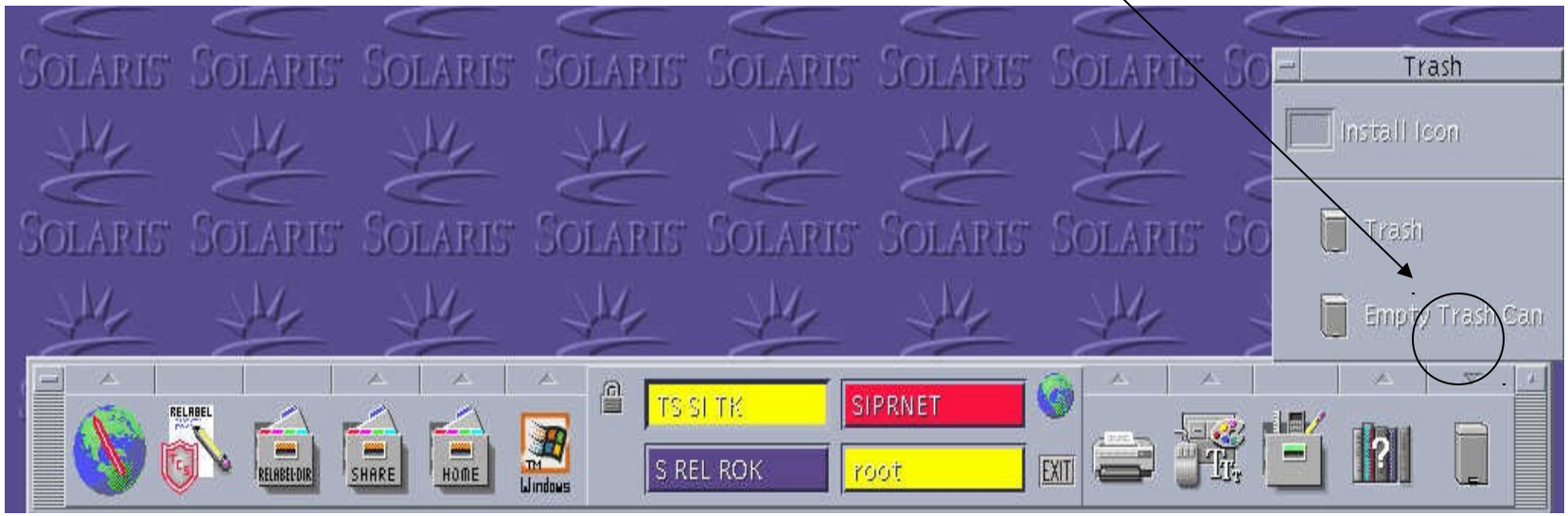


1. Click here to get the pop up menu

Share Directory File Manager



- Trash Can
  - Drag and drop file icons onto trash can to delete
  - Permanently delete files by emptying trash can
    - Left single-click on trash can menu.
      - » Select **Empty Trash Can**

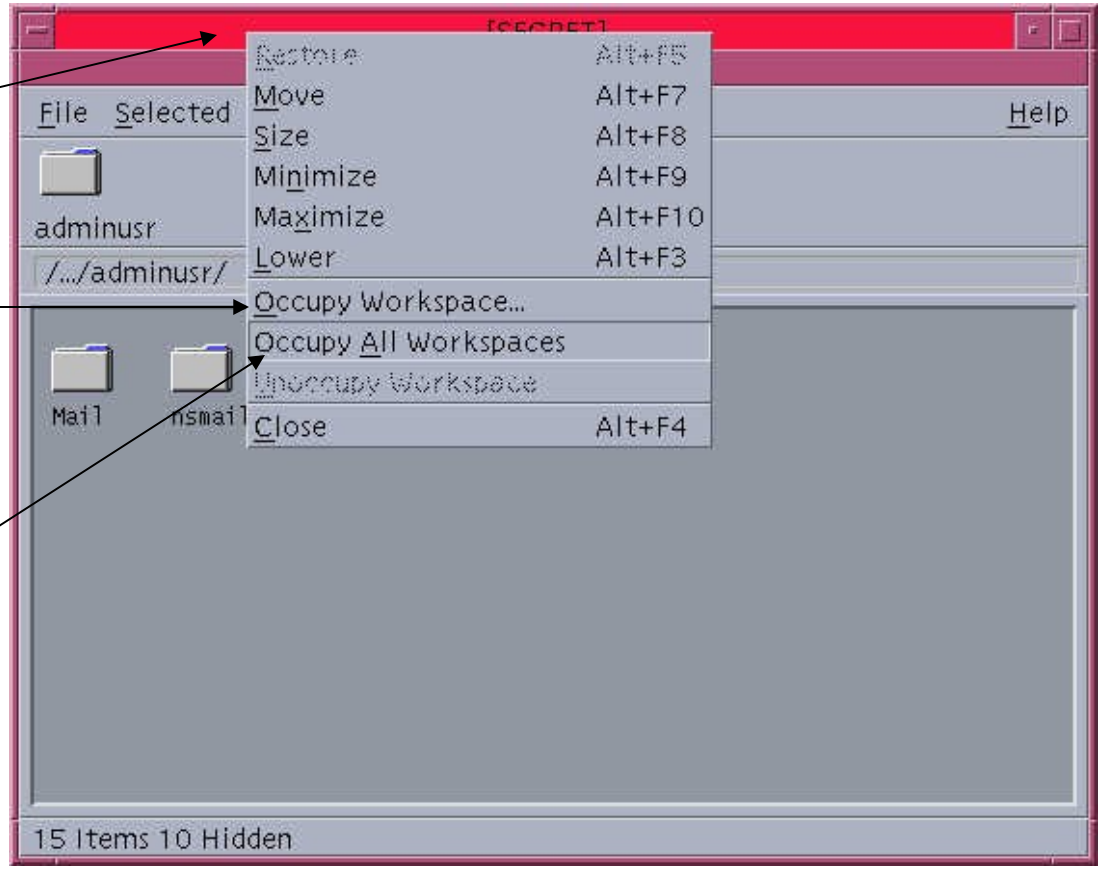


- Screen Locking
  - Select the screen lock icon on the CDE panel with a single left click. Screen Lock will execute, requires password to unlock. If the user leaves the SecureOffice terminal for any reason, execute the screen lock mechanism prior to removing the users smart card

- Logging out
  - Select the **Exit** icon on the CDE panel with a single left click
  - Select '**OK**' at the logout confirmation dialog

Moving Windows between workspaces

- Right click on the SL portion of the window
- Select **Occupy Workspace** and you will be prompted for the appropriate workspace.
- Select **Occupy All Workspaces** if you want the window in all workspaces.

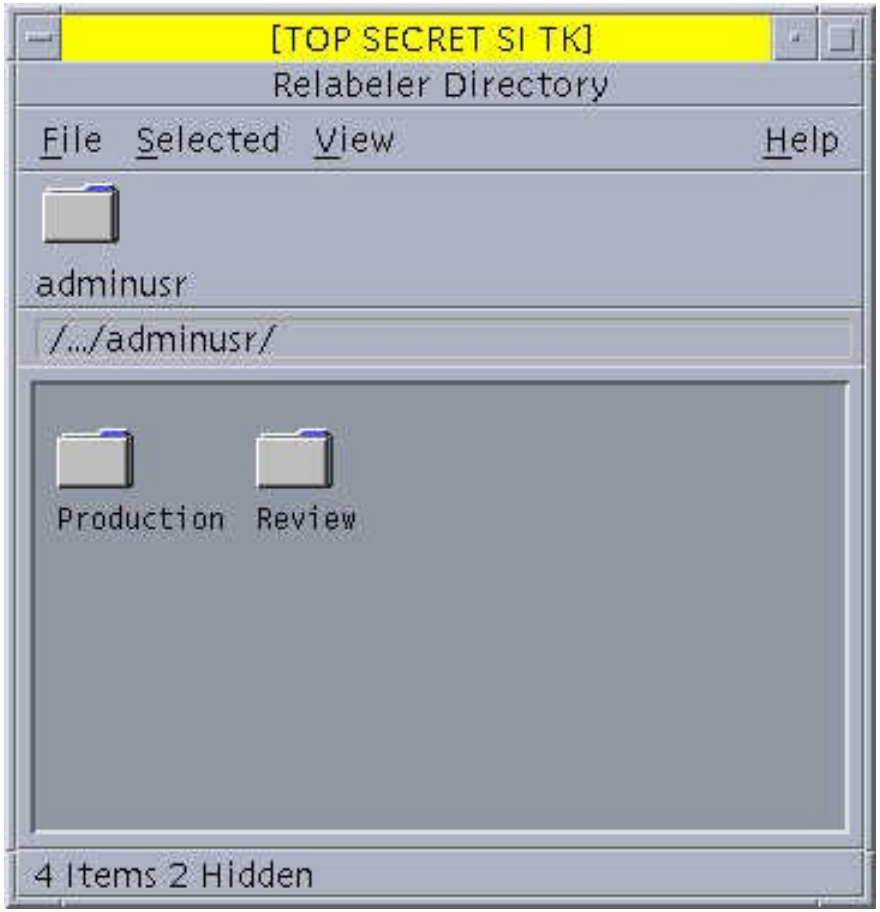


- Relabeling Files
  - To change the classification label of a file, you must use the TCS **Trusted File Relabeler** application
    - Upgrades and Downgrades
    - All transfers are audited
    - All transfers are Virus Scanned
  - Files must be put into staging area for relabeling
    - drag/drop file icon on any of the **Relabeler icons** (CDE Front Panel or Application Manager)
    - Can also right click a data file and select copy to relabeler
  - Click the **Relabeler icon** (desktop or front panel) to launch

- Relabel Directory

Note: Directories are not created until accessed by user

- Users Home Directory
- Production
  - Store files for Relabeling
- Review
  - Only if user is an authorized Reviewer
- Released
  - Only in destination SL's
  - Files are stored in this directory after they are reviewed

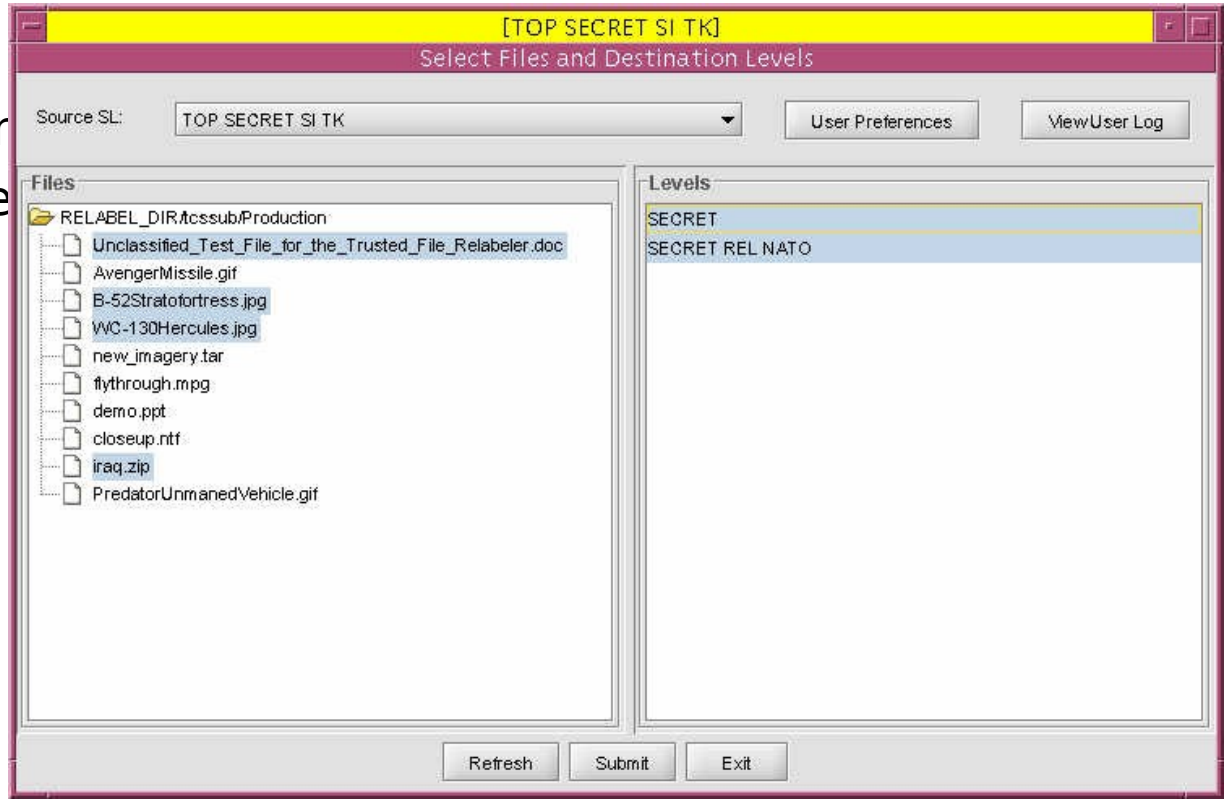


SecureOffice User
File Movement

- Trusted File Relabeler Roles
  - **Submitter**
    - Minimal privilege user
    - Allowed to submit files as a recommendation for further processing
    - Selects file(s) and destination Security Levels
  - **Processor**
    - Subject Matter Expert, Information Transfer Agent
    - Allowed to process files for relabeling (virus scan, dirty word search, etc)
    - Selects file(s) and destination Security Levels
  - **Reviewer**
    - Validates the Processor functions
    - Final release authority for file transfer to the selected destination Security Levels

SecureOffice User
File Movement

- Submitter Start Screen
  - Main Window
  - Source SL dropdown
  - Files – all files in the user's Production directory
  - Levels – select destination SL's

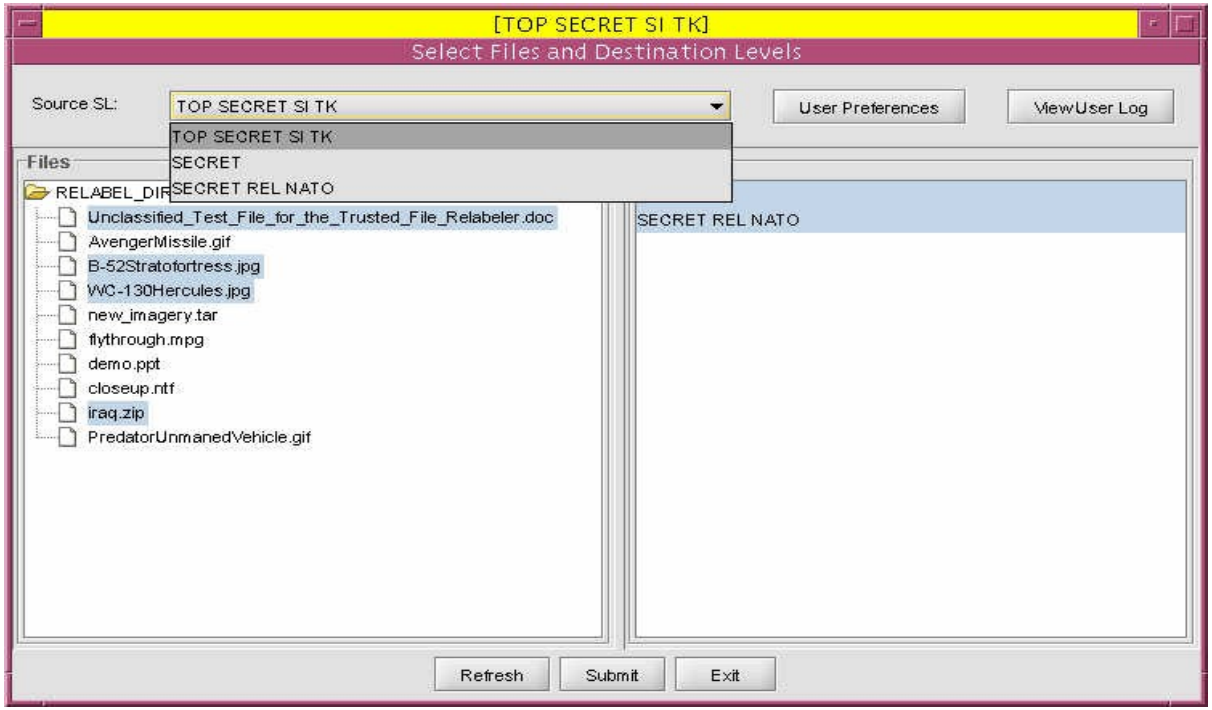


SecureOffice User
File Movement

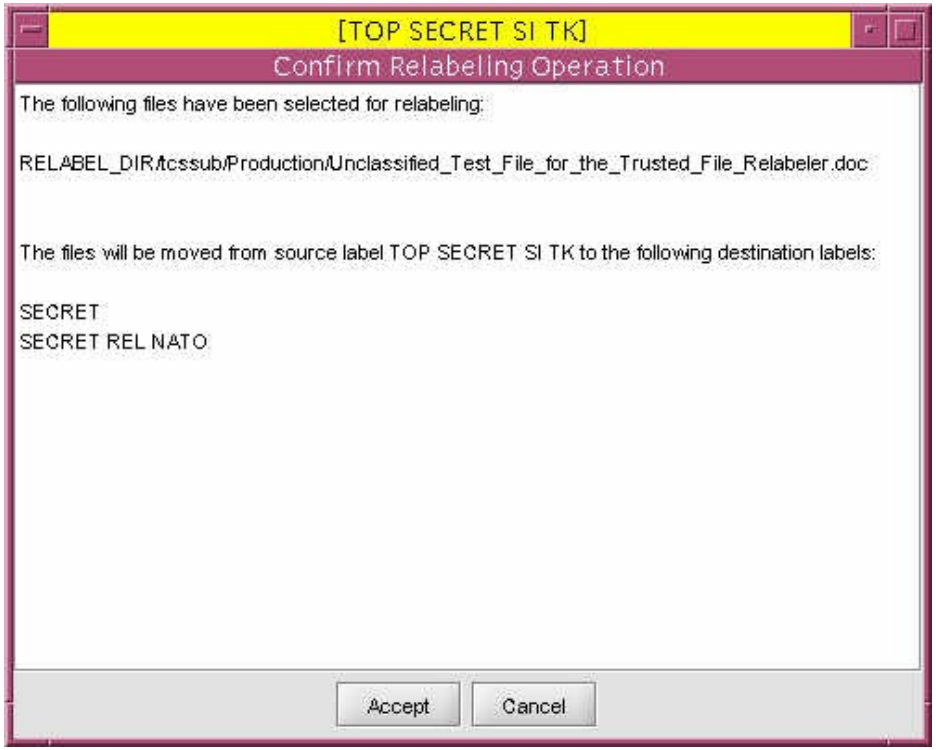
- User Preferences
  - Sets up default user configuration
  - Delete Source Files Automatically
    - Removes all Files after Processing
  - Do Not Display Confirmation
    - Reduces the number of dialog boxes
  - Default Source SL
  - Default Role/Function
    - If a user has access to more than one role, sets default

SecureOffice User
File Movement

- Select Source SL
  - Dropdown list of all available source SL's
  - Changes file list to appropriate Production directory



- Confirmation Dialog
  - Shows files selected for relabeling and the destination SL's for those files



- Comments
  - Allows Submitter to enter text comments concerning the files to the Processor (optional)
  - Allows Submitter to enter a file bundle title (mandatory)

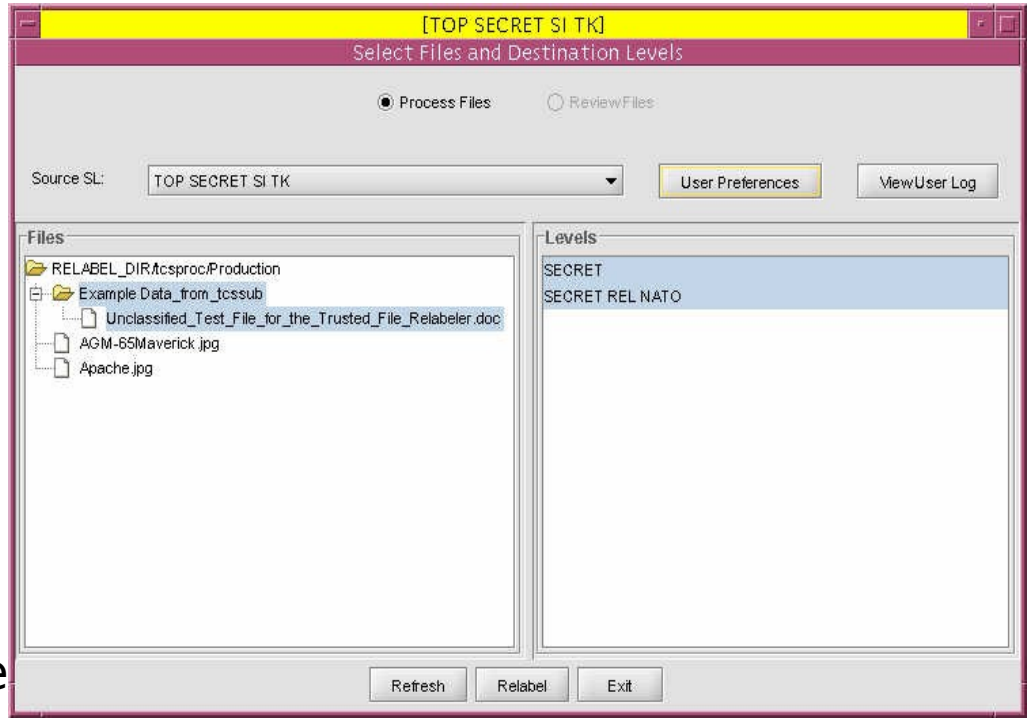
- Select Processor
  - Allows Submitter to select the appropriate Processor (mandatory)
  - This completes the Submitter role responsibilities

SecureOffice User
File Movement

- Processor Start Screen

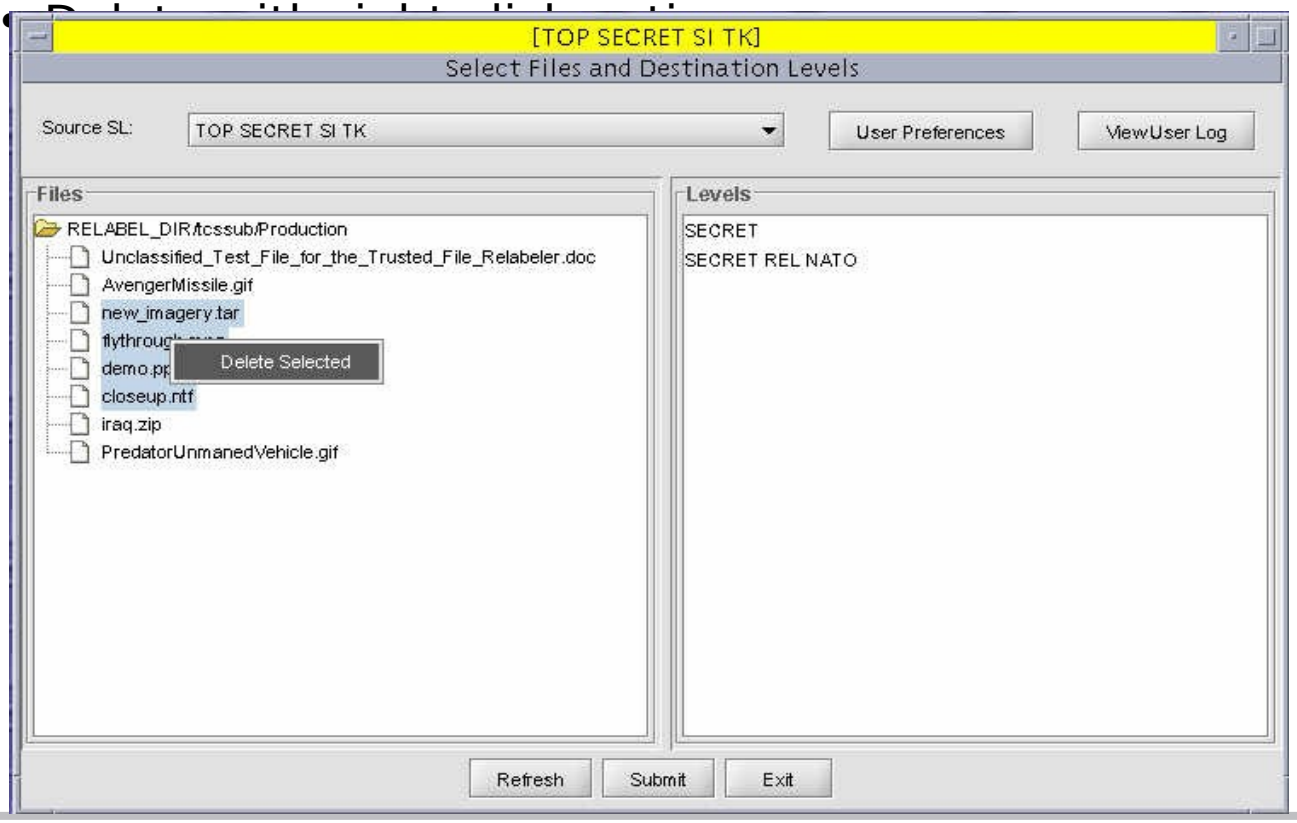
Note: This is a different user/role

- Shows contents of Production directory (left side)
- Select destination SL's (right side)
- Processor can modify the files selected and/or the destination Security Levels selected by the submitter
- Processor can also initiate file transfer



SecureOffice User
File Movement

- Delete Selected Files
  - All roles can select files or file bundles (select multiple with CTRL)

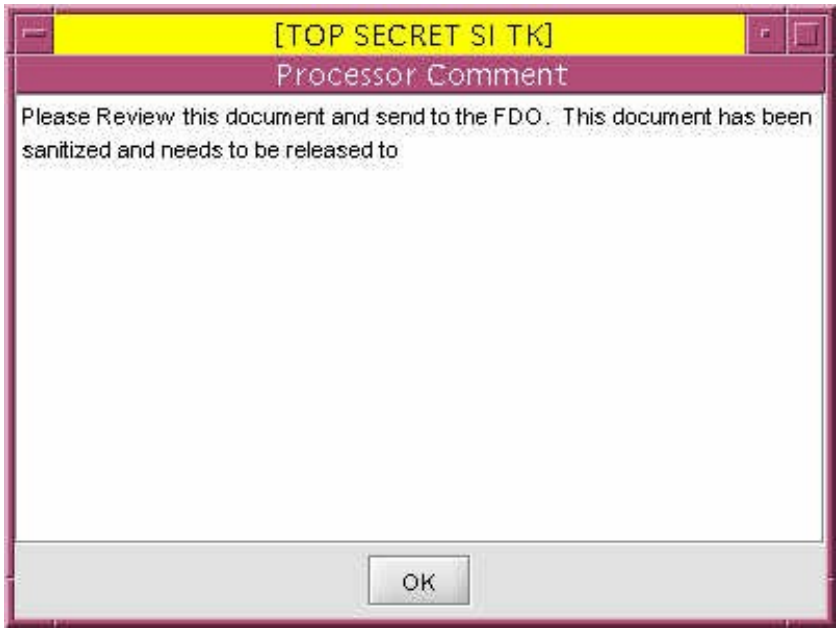


- File Type and Virus Scanning Status Bar
  - Progress bar for virus scanning file(s) and file typing
  - File type check verifies against system-wide default file typing policy

- Dirty Word Search Progress Bar
  - Progress bar for conducting file dirty word search
  - Checks file(s) against system Dirty and Clean word lists

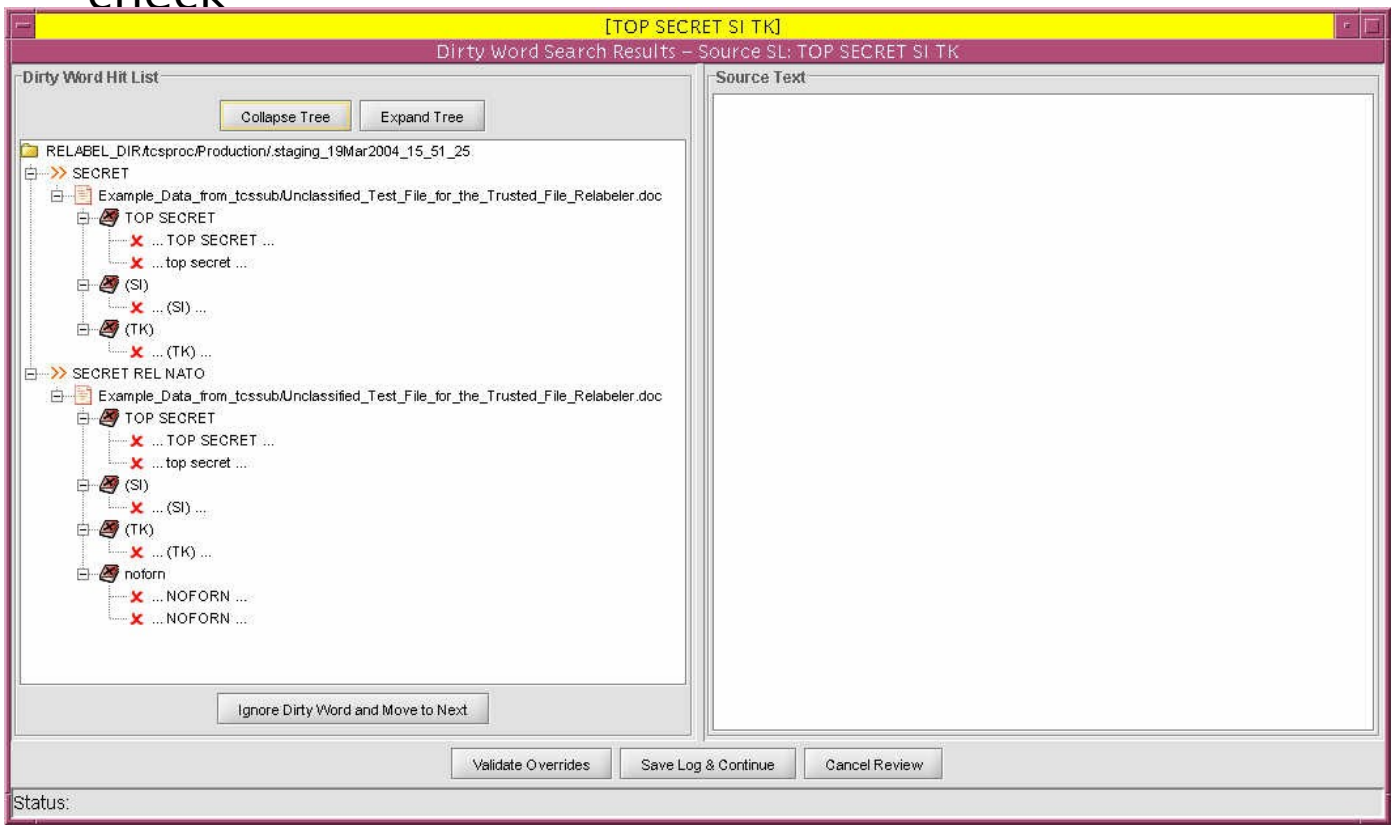
- Select Destination SL Warning
  - Processor MUST select at least one destination SL

- Review Submitter Comments
  - Review Comments by right-clicking the file bundle
  - Select View Comments



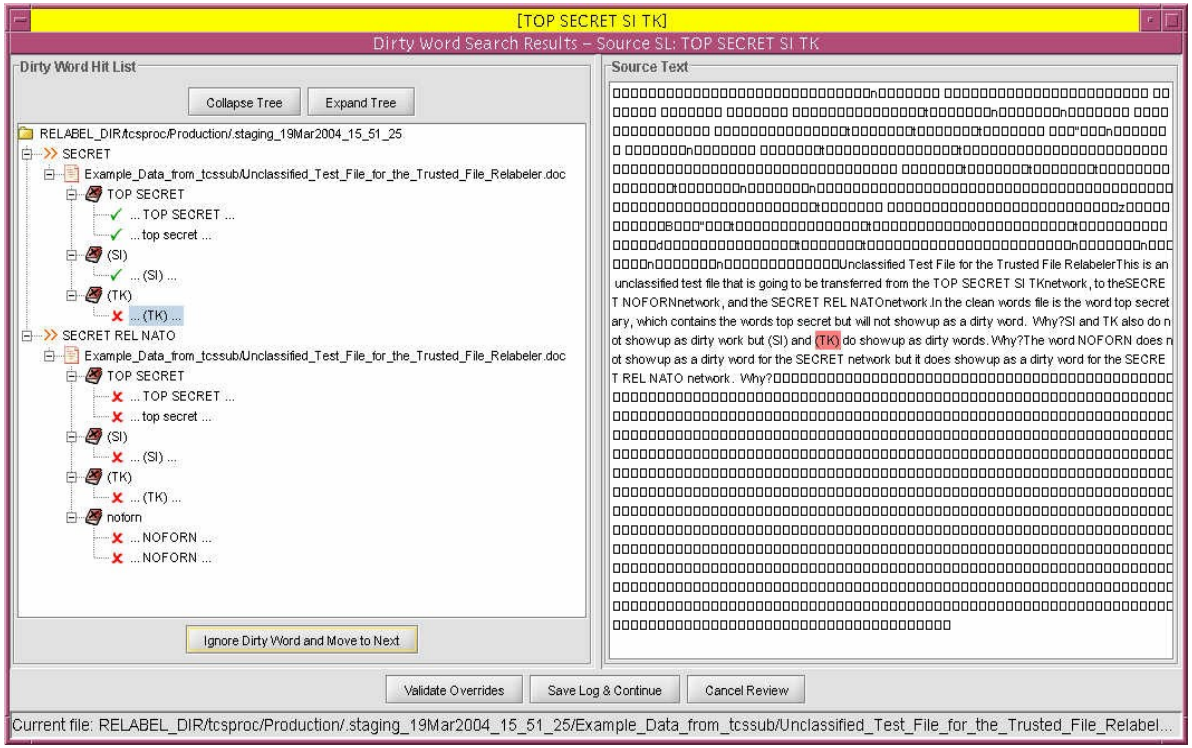
SecureOffice User
File Movement

- Dirty Word Search Engine
  - Main screen appears after Virus Scan and File Type policy check



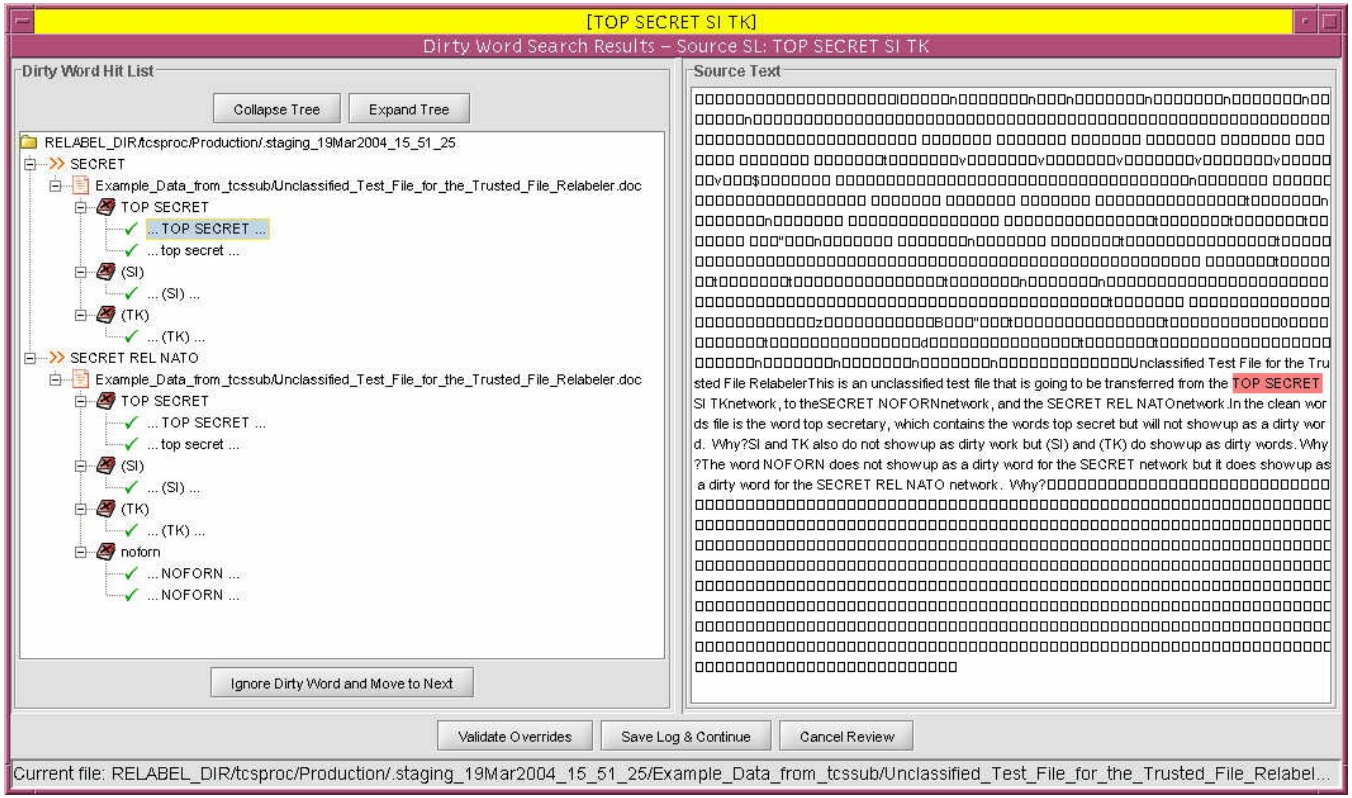
SecureOffice User
File Movement

- Dirty Word Search Engine
  - Dirty Words highlighted
  - Unreviewed dirty words annotated with red **X**
  - Overridden words annotated with green ✓
  - Only false positives should be overridden



- Dirty Word Engine
  - Navigate by clicking on left-side dirty word occurrences
  - Dirty words will be highlighted in text (right-side)
  - All dirty words must be overridden to continue
  - If a word is not a false positive, cancel the operation and modify the file in its native format

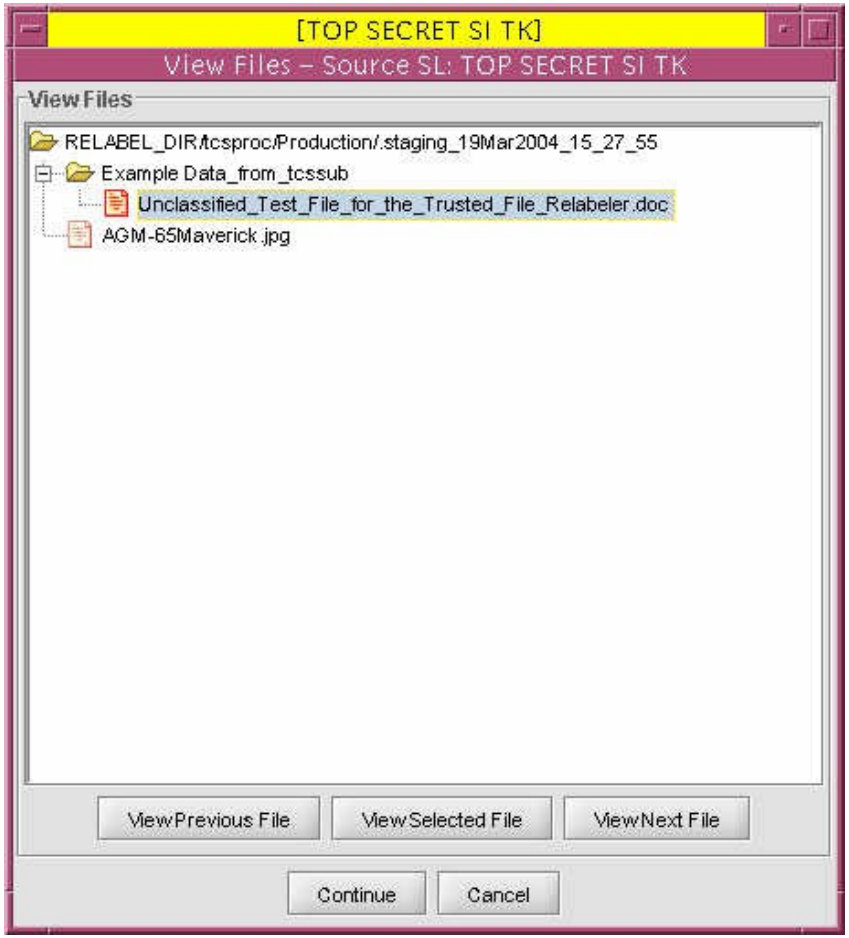
- Dirty Word Search Engine
  - All Dirty Words overridden (False Positives)



- Validate Dirty Word Search
  - Validate Overrides button checks file(s) to ensure that all dirty word hits have been overridden

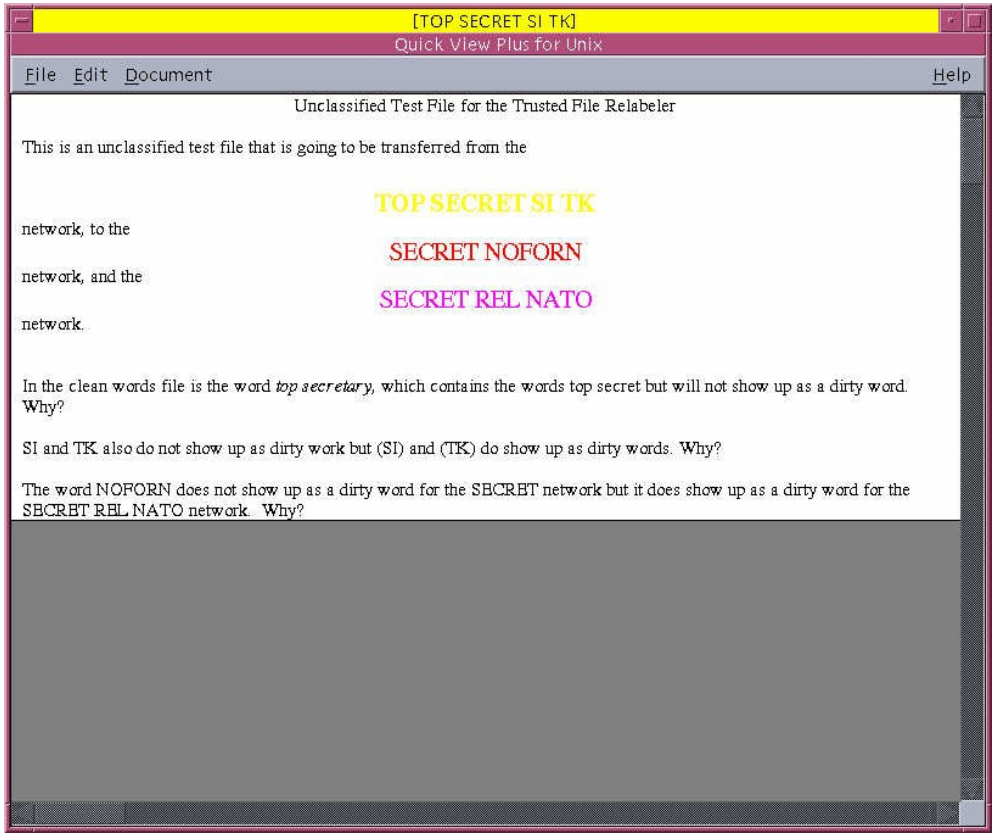
- Save Dirty Word Search Scan
  - Save Log and Continue button generates an XML file containing all dirty words and decisions
  - File accompanies Relabel bundle to Reviewer for verification

- File Viewer
  - Optional step, determined by system policy (typically enforced)
  - View files by
    - Double-click file name
    - Single-click file name and click View Selected File
    - Click View Next File
  - When all files are reviewed (green icon), click Continue



SecureOffice User
File Movement

- QuickView Plus
  - Native file viewer for MS documents (Word, PowerPoint, Excel, etc)
  - Once the file has been reviewed, close the application to continue
  - When the above is complete, the file icon in the File Viewer dialog will turn from red to green

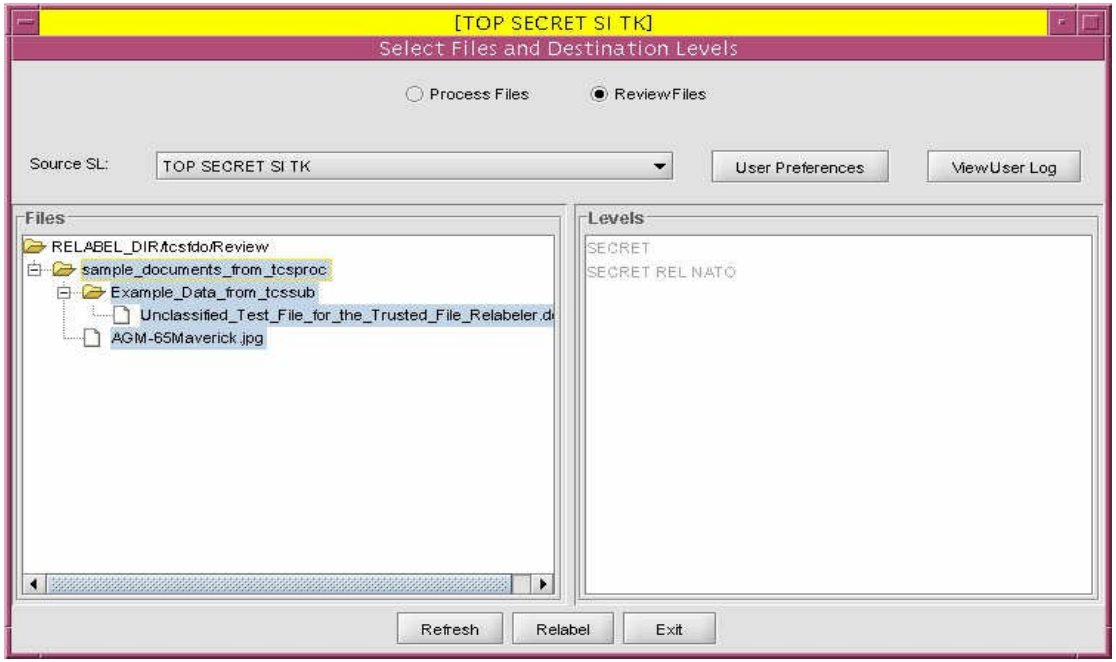


- Comments
  - Allows Processor to enter text comments concerning the files to the Reviewer (optional)
  - Allows Processor to select appropriate Reviewer (drop down list)
  - Allows Processor to enter a file bundle title (mandatory)
  - This step completes the Processor role responsibility

- Reviewer Start Screen

Note: This is a new user/role

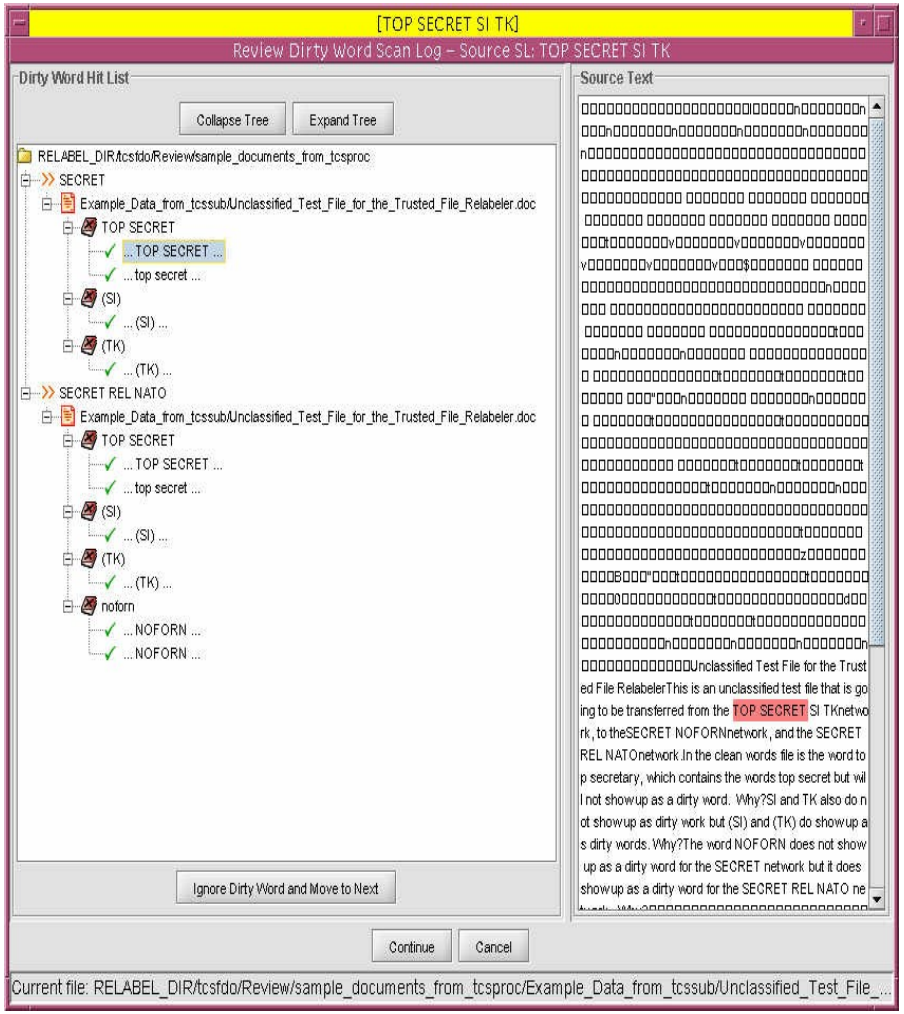
- Main window for Reviewer role
- Note Review Files radio button selected



- Reviewer Role Function
  - Select any file bundle sent for review
  - Right-click to select View Comments
  - Note: Destination SL’s are static, and cannot be modified by Reviewer

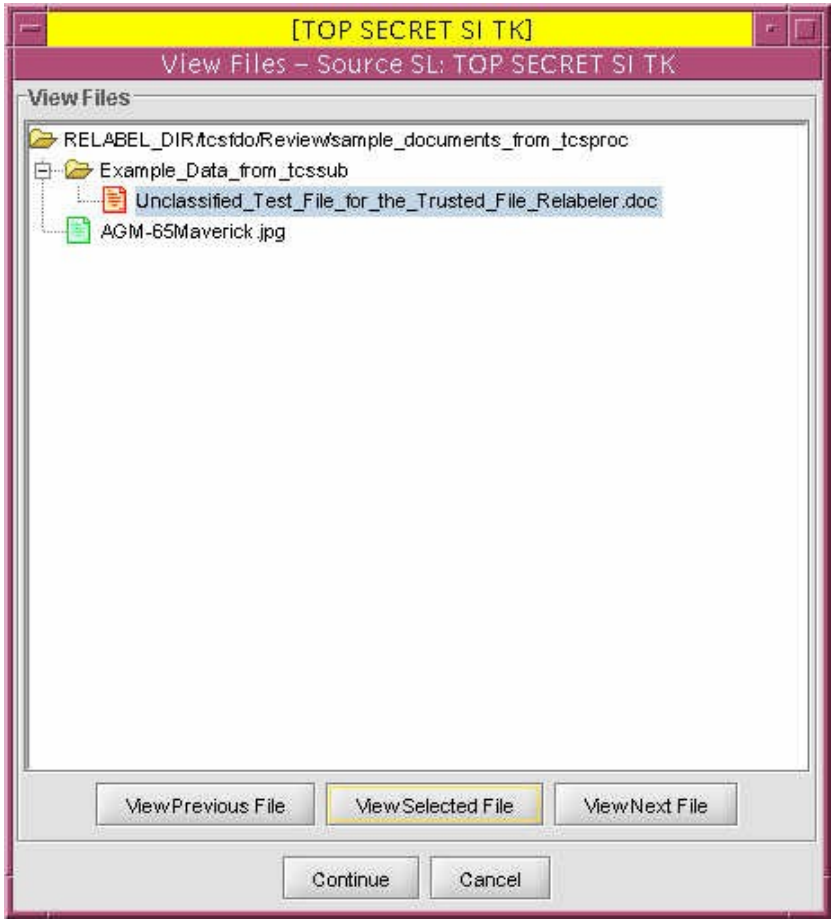
SecureOffice User
File Movement

- Dirty Word Search Review
  - Results from Processor Dirty Word Engine presented
  - Reviewer cannot modify any Processor decisions
  - If Reviewer does not agree with Processor decisions, Cancel and inform Processor to modify files and re-submit

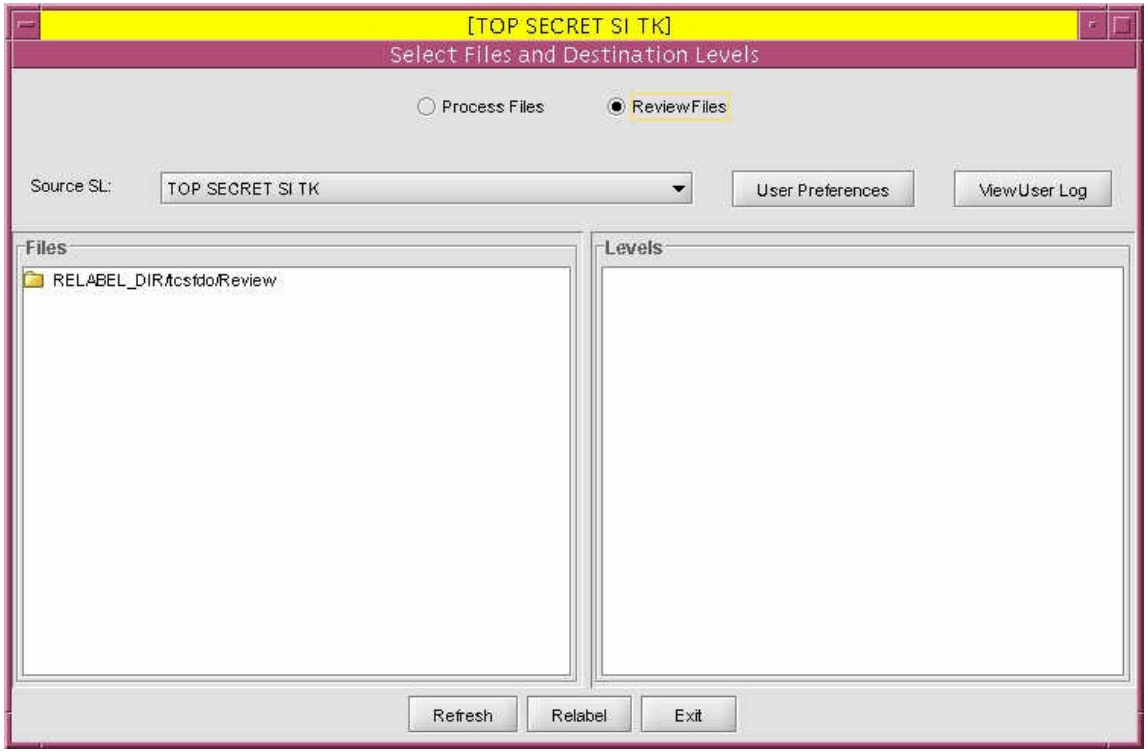


SecureOffice User
File Movement

- File Viewer
  - View files by
    - Double-click file name
    - Single-click file name and click View Selected File
    - Click View Next File
  - When all files are reviewed (green icon), click Continue
  - Note: All files being processed may only be viewed. They are opened read-only during the Relabel process.

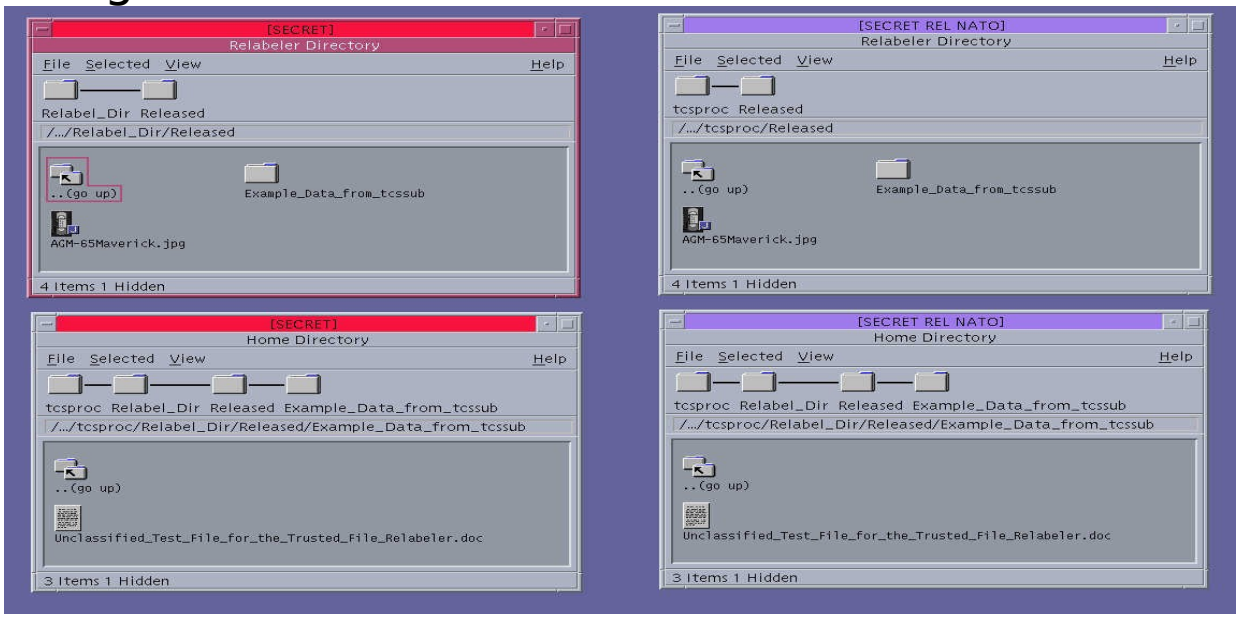


- Review Complete
  - When File Review is complete, a confirmation dialog appears and the Reviewer Main window returns



SecureOffice User
File Movement

- Multi-Level Released Directories
  - File must be successfully Reviewed and Released
  - Files are placed in Processors Released directory at the appropriate SL
  - Ensure that the appropriate Security Level is selected when locating Relabeled files



Dirty Words

Word as normally found in text	TOP SECRET
Word with embedded blanks	T O P S E C R E T
Two-line header or footer	TOP SECRET
Word embedded in other words	stop secreting

- Supplemental Dirty Words
  - Destination Level specific dirty words
  - Allows for fine-tuned Dirty Word List
  - Administratively controlled

- Clean Words
  - Exclusion list for Dirty Word engine
  - Allows for elimination of false positives
  - Administratively controlled
  - Example:
    - Dirty Word – TOP SECRET
    - Clean Word – top secretary
    - The phrase ‘top secretary’ contains the Dirty Word TOP SECRET, but is not returned to the user as it is explicitly called out in the Clean Word list

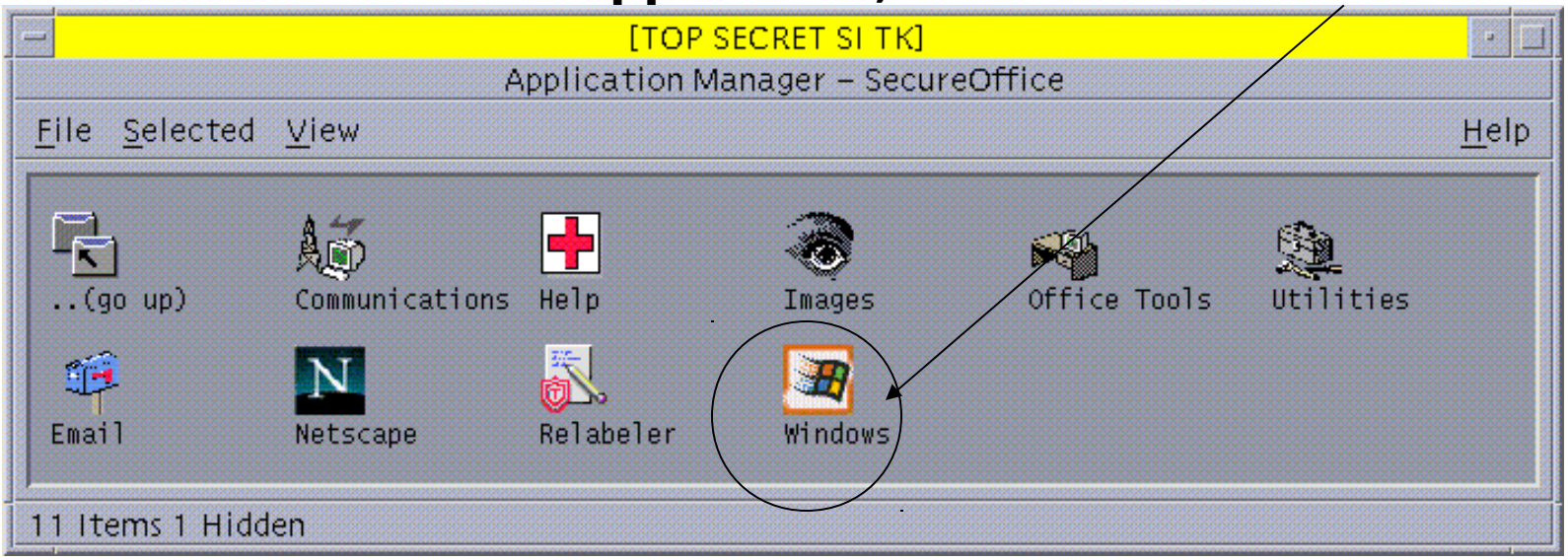
- Supplemental Clean Words
  - Destination Level specific Clean Word list
  - Allows for fine-tuned Clean Word list
  - Administratively controlled

- Relabeling Files (con't)
  - Relabeled files can be e-mailed or ftp'd
  - Relabeled files can be found by accessing the Relabel Dir icon on the CDE Front Panel and opening the Released folder
  - File location: /export/home/Relabel_Dir/ $USERNAME/Released
  - Remember to access the directory at the level of the relabeled file

- Citrix Metaframe
  - Introduction
  - Using Citrix Metaframe
    - Starting/Stopping
    - Login/Logoff Citrix Metaframe Servers
    - Shared Drives
      - » Windows Drives
      - » UNIX Directories
    - Copy/Cut/Paste Between Windows and Unix environments
      - » Not currently supported for accreditation reasons

Windows Citrix Metaframe

To start Citrix client application, left double click on Windows



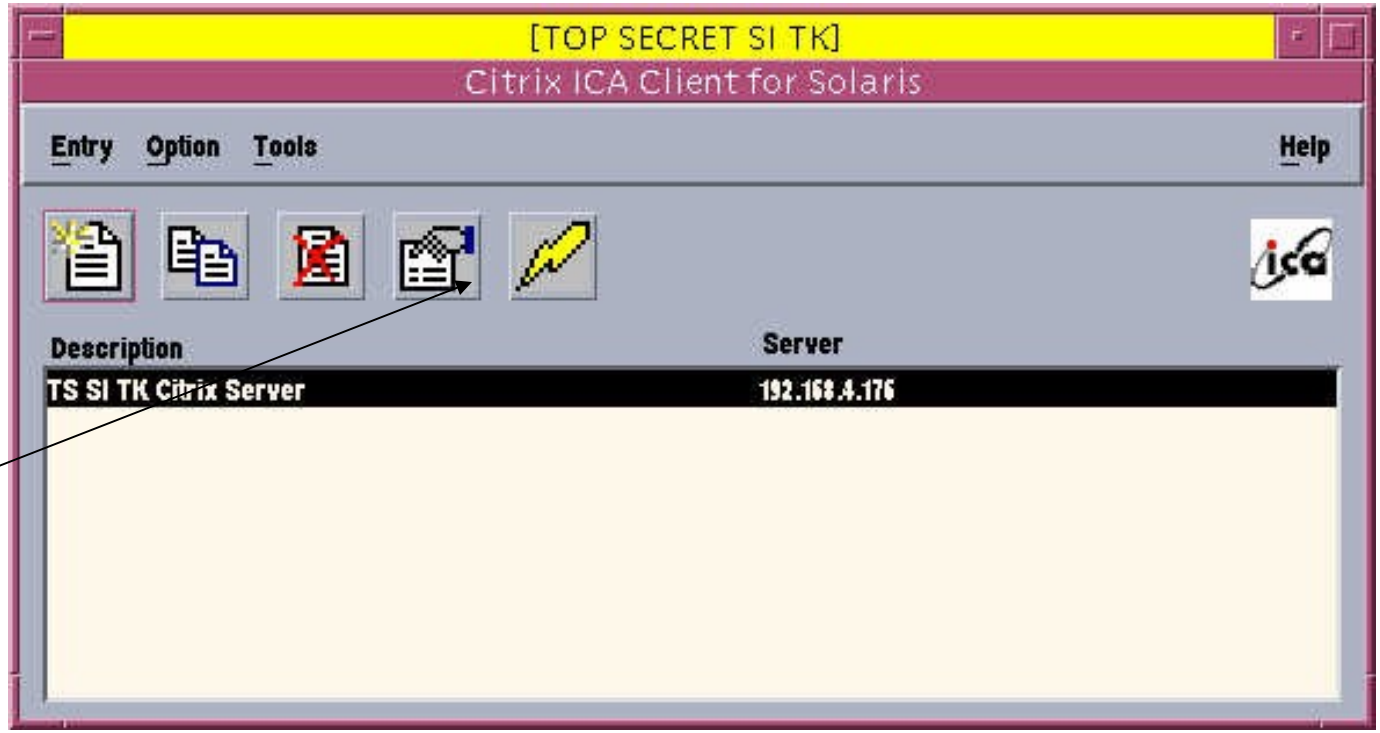
Or, if properly configured, single-click on the Windows icon on the CDE Front Panel.

Citrix Metaframe
Starting Client Connection

Double click on selected server to start connection

- OR -

Select Server with one left click then left click on connection icon

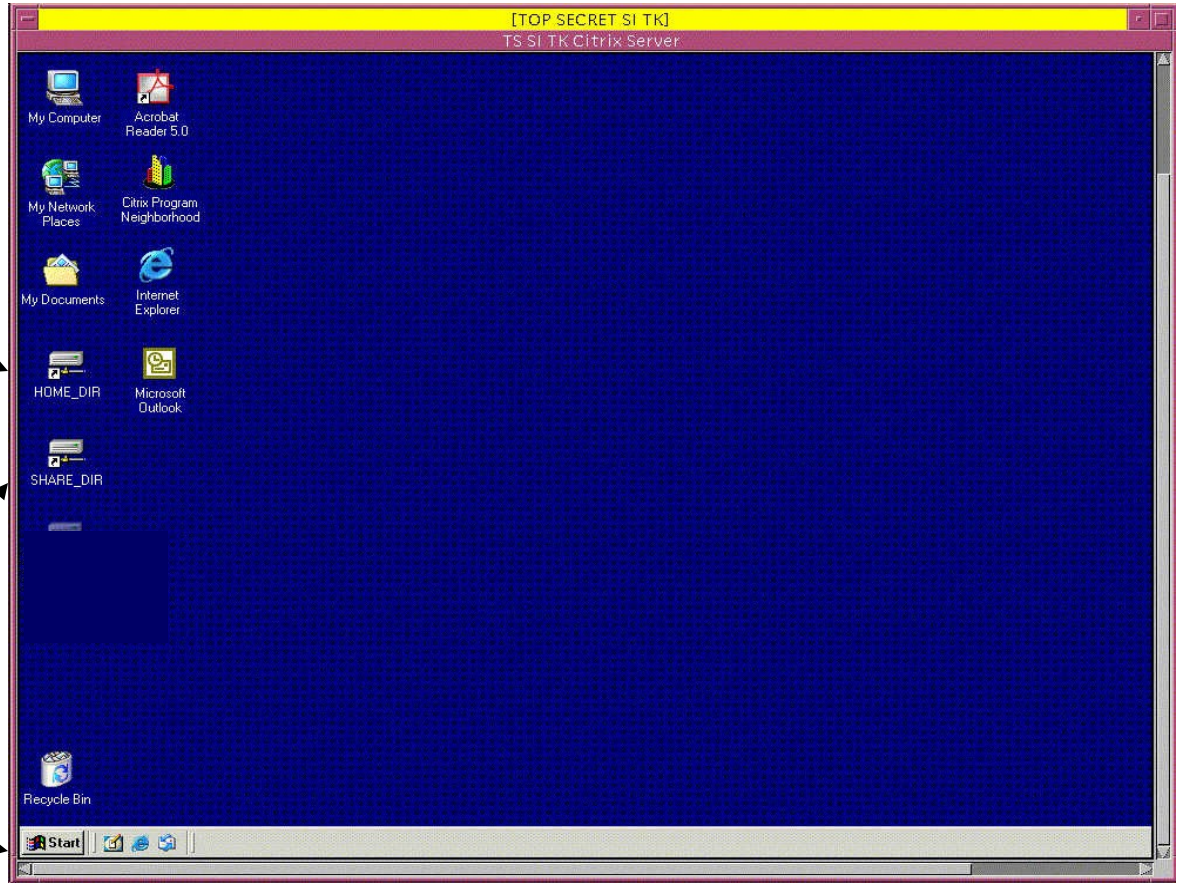


Citrix Metaframe
Starting Client Connection

Client will attempt to connect to Citrix Server at specified SL. This will take a moment.

Citrix Metaframe Desktop Window

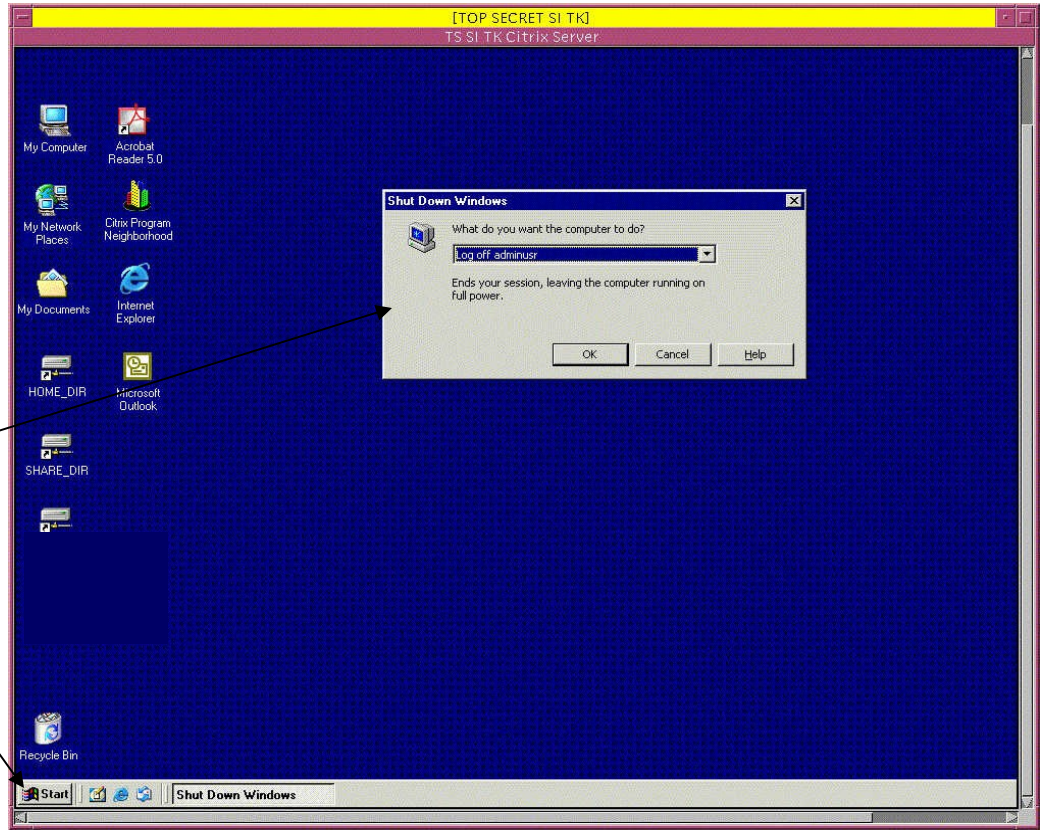
- UNIX Home Directory
  - Access to Relabel Directories
- UNIX Share Directory
- Windows Start Menu



Citrix Metaframe
Logging Off Citrix Server

- Left Click **Start** menu and select **Shutdown**

- Select **Logoff *username***

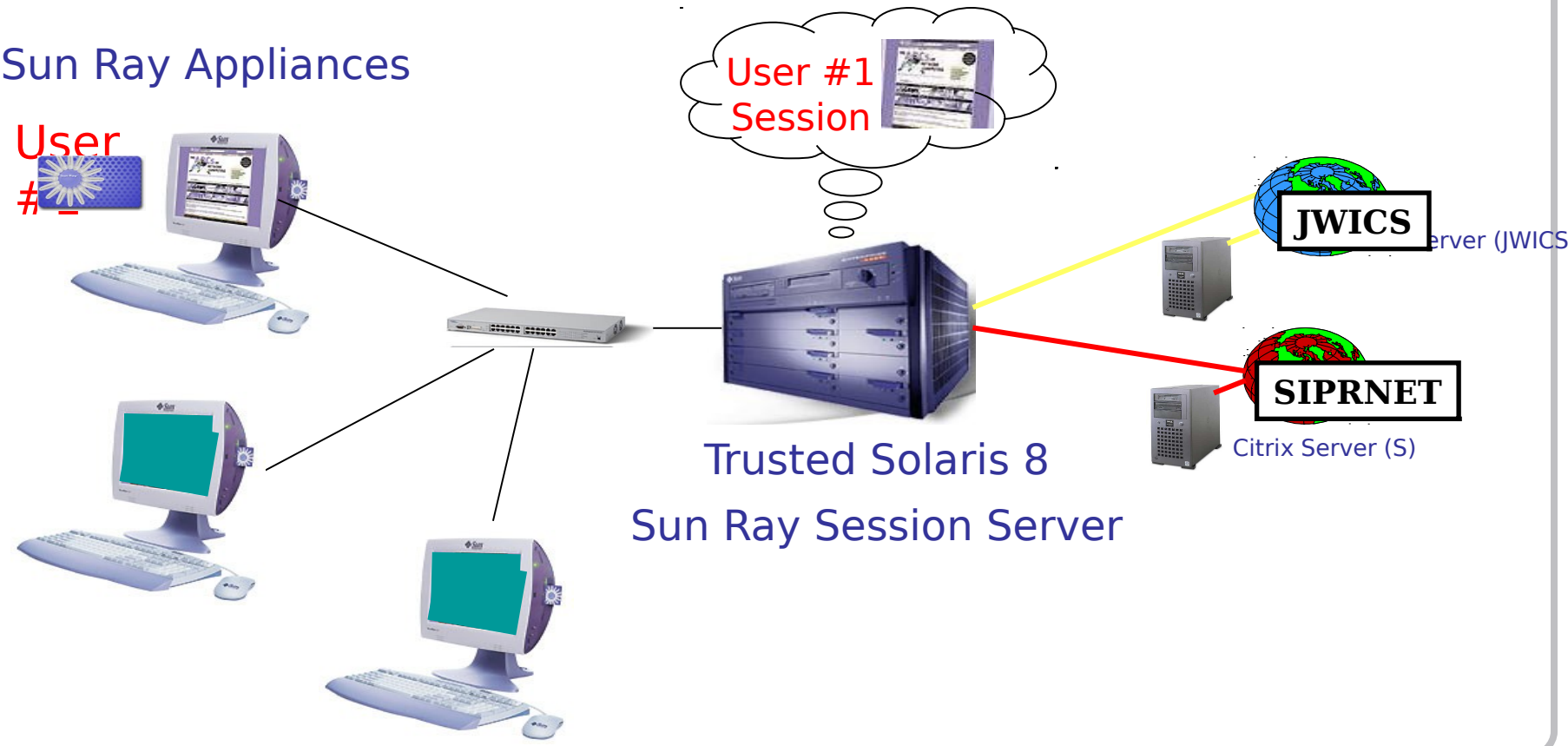


SecureOffice User

- Integrated Hardware
  - SecureOffice Configuration
    - Introduction
      - Specialized Sun Diskless WorkStations
      - User session is executed on Sun Ray Session Server and displayed on SunRay Workstation
      - SunRay appliance is optionally configured to require a registered Smartcard for access.
      - User has access to all networks connected to SunRay Session Server

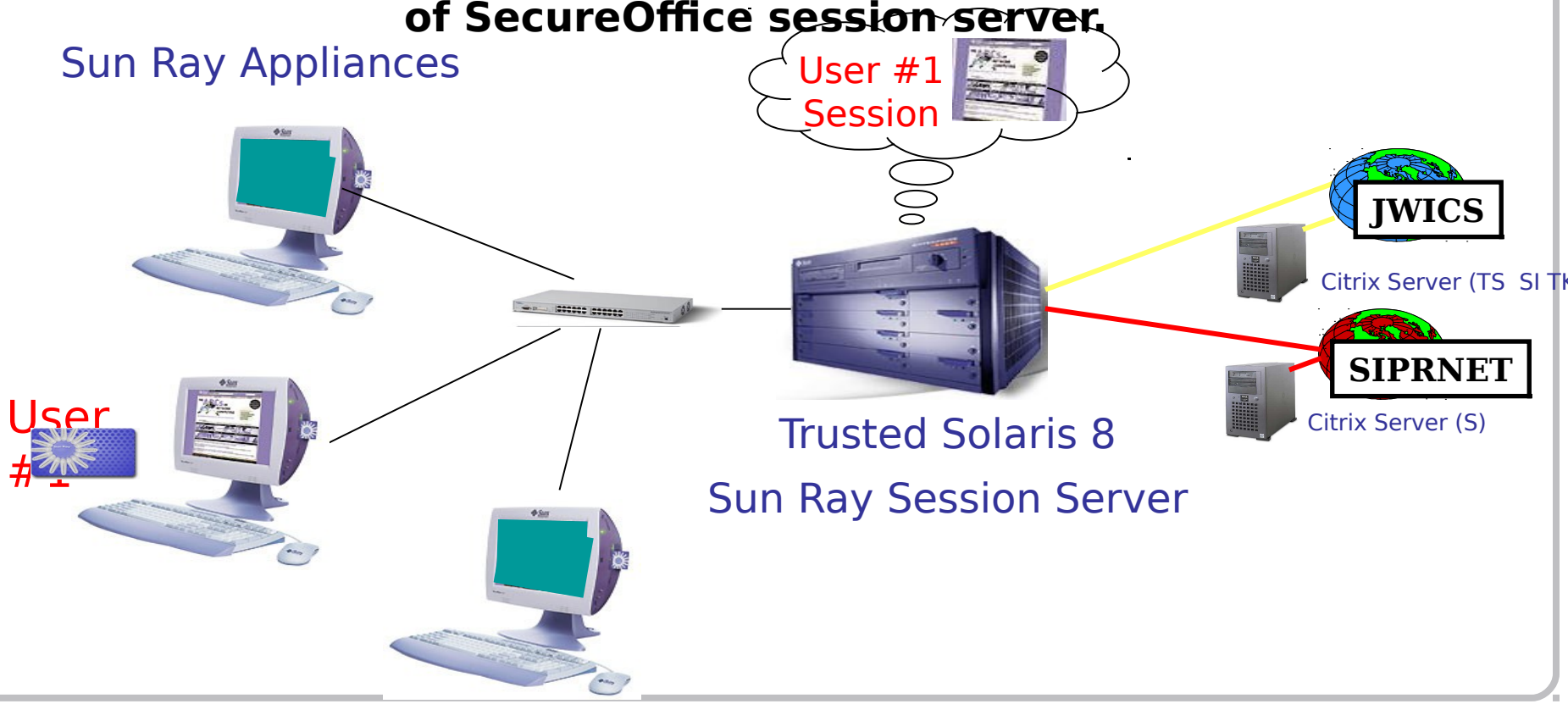
Sun Ray "Hot Desk" Demonstration

User Inserts registered smartcard, logs in and starts a session



Sun Ray "Hot Desk" Demonstration

User removes registered smartcard, inserts into an unused workstation. Users session moves with smartcard until user logs off of SecureOffice session server.



SecureOffice User
Course Review

- Trusted Operating System Overview
- Desktop Features and Conventions
- File Movement
- Integrated Applications
- Integrated Hardware

- Questions?